Ogłoszenie o zamówieniu
Dostawy
ZAKUP I DOSTAWA SPRZĘTU INFORMATYCZNEGO, OPROGRAMOWANIA WRAZ Z LICENCJAMI

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ SANATORIUM UZDROWISKOWE MINISTERSTWA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI "AGAT" W JELENIEJ GÓRZE

1.3.) Oddział zamawiającego: SP ZOZ Sanatorium Uzdrowiskowe MSWiA "AGAT" w Jeleniej Górze

1.4) Krajowy Numer Identyfikacyjny: REGON 230081055

1.5) Adres zamawiającego

1.5.1.) Ulica: ul. Cervi 14

1.5.2.) Miejscowość: Jelenia Góra

1.5.3.) Kod pocztowy: 58-560

1.5.4.) Województwo: dolnośląskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL515 - Jeleniogórski

1.5.9.) Adres poczty elektronicznej: sekretariat@sanatorium-agat.pl

1.5.10.) Adres strony internetowej zamawiającego: www.sanatorium-agat.pl

1.6.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - samodzielny publiczny zakład opieki zdrowotnej

1.7.) Przedmiot działalności zamawiającego: Zdrowie

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:

ZAKUP I DOSTAWA SPRZĘTU INFORMATYCZNEGO, OPROGRAMOWANIA WRAZ Z LICENCJAMI

2.4.) Identyfikator postępowania: ocds-148610-118b382d-7e1f-40df-a4fe-b64355b3054e

2.5.) Numer ogłoszenia: 2026/BZP 00228868

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2026-05-05

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2026/BZP 00029168/02/P

2.10.) Identyfikator pozycji planu postępowań:

1.2.1 Zestaw urządzeń informatycznych

2.11.) O udzielenie zamówienia mogą ubiegać się wyłącznie wykonawcy, o których mowa w art. 94 ustawy: Nie

2.14.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Nie

2.16.) Tryb udzielenia zamówienia wraz z podstawą prawną

Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA III – UDOSTĘPNIANIE DOKUMENTÓW ZAMÓWIENIA I KOMUNIKACJA

3.1.) Adres strony internetowej prowadzonego postępowania
https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-118b382d-7e1f-40df-a4fe-b64355b3054e

3.2.) Zamawiający zastrzega dostęp do dokumentów zamówienia: Nie

3.4.) Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej: Tak

3.5.) Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami - adres strony internetowej: https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-118b382d-7e1f-40df-a4fe-b64355b3054e

3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej: 1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem https://ezamowienia.gov.pl.
2. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
3. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu „Wykonawca” na Platformie e- Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej https://ezamowienia.gov.pl oraz informacje zamieszczone w zakładce „Centrum Pomocy”.
4. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania.
5. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
6. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
7. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (22) 458 77 99 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej https://ezamowienia.gov.pl w zakładce „Zgłoś problem”.

3.8.) Zamawiający wymaga sporządzenia i przedstawienia ofert przy użyciu narzędzi elektronicznego modelowania danych budowlanych lub innych podobnych narzędzi, które nie są ogólnie dostępne: Nie

3.12.) Oferta - katalog elektroniczny: Nie dotyczy

3.14.) Języki, w jakich mogą być sporządzane dokumenty składane w postępowaniu:

polski

3.15.) RODO (obowiązek informacyjny): 1. Administratorem Pani/Pana danych osobowych jest Samodzielny Publiczny Zakład Opieki Zdrowotnej Sanatorium Uzdrowiskowe MSWiA “AGAT”, z siedzibą w 58-560 Jelenia Góra ul. Cervi 14 adres e-mail: sekretariat@sanatorium-agat.pl , tel. +48 75 75 520 64 .
2. Może Pan/Pani kontaktować się w sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących na mocy RODO z Administratorem z wykorzystaniem powyższych danych teleadresowych lub z wyznaczonym u Administratora Inspektorem ochrony danych na adres e-mail: iod@sanatorium-agat.pl
3.Pani/Pana dane niezbędne do udziału w postępowaniu będą przetwarzane w celu związanym z realizacją postępowania o udzielenie zamówienia publicznego na podstawie ustawy Prawo zamówień publicznych oraz działanie przez administratora w interesie publicznym [PZP], zgodnie z art. 6 ust. 1 lit. c, e oraz art. 10 RODO .
4.Pani/Pana dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymywania na podstawie przepisów prawa lub umowy, w tym: podwykonawcom, firmom zapewniającym niszczenie dokumentów i nośników danych, biurom obsługi prawnej, itp.
5.Ze względu na jawność postępowania o udzielenie zamówienia publicznego, odbiorcami Pani/Pana danych osobowych mogą być wszystkie zainteresowane osoby lub podmioty. Ograniczenie dostępu do danych może wystąpić jedynie w szczególnych przypadkach, jeśli jest to uzasadnione ochroną prywatności, interesem publicznym lub informacja stanowi tajemnicę przedsiębiorstwa.
6.W związku z jawnością postępowania o udzielenie zamówienia publicznego Pani/a dane mogą być także przekazywane do państw trzecich.
7.Podanie przez Panią/Pana danych osobowych jest wymagane przepisami PZP do wzięcia udziału w postępowaniu.
8.Posiada Pani/Pan prawo do wniesienia skargi do Prezesa UODO (www.uodo.gov.pl) w razie uznania, że przetwarzanie danych przez Administratora narusza przepisy prawa.
9.Pani/Pana dane osobowe w przypadku postępowań o udzielenie zamówienia publicznego będą przechowywane przez okres oznaczony kategorią archiwalną wskazaną w Jednolitym Rzeczowym Wykazie Akt , który zgodnie z art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164) został przygotowany w porozumieniu Naczelnym Dyrektorem Archiwów Państwowych.10.Posiada Pan/Pani: na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
• na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą PZP oraz nie może naruszać

integralności protokołu postępowania oraz jego załączników;
• na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO]
• prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
nie przysługuje Pani/Panu:
•w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych; prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO; 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

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Informacje ogólne odnoszące się do przedmiotu zamówienia.

4.1.1.) Przed wszczęciem postępowania przeprowadzono konsultacje rynkowe: Nie

4.1.2.) Numer referencyjny: 1/2026

4.1.3.) Rodzaj zamówienia: Dostawy

4.1.4.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Tak

4.1.8.) Możliwe jest składanie ofert częściowych: Tak

4.1.9.) Liczba części: 6

4.1.10.) Ofertę można składać na wszystkie części

4.1.11.) Zamawiający ogranicza liczbę części zamówienia, którą można udzielić jednemu wykonawcy: Nie

4.1.13.) Zamawiający uwzględnia aspekty społeczne, środowiskowe lub etykiety w opisie przedmiotu zamówienia: Nie

4.2. Informacje szczegółowe odnoszące się do przedmiotu zamówienia:

Część 1

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 1- SERWER WIRTUALIZACYJNY – 1 SZTUKA
Obudowa Obudowa Rack o wysokości max. 1U z możliwością instalacji min. 8 dysków 2,5” SATA z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 304 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla jednego procesora. Dla oferowanego serwera.
RAM Min. 256GB DDR5 RDIMM 6400MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 2TB pamięci RAM.
Zabezpieczenia pamięci RAM Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection
Gniazda PCIe - minimum dwa sloty PCIe x16 generacji 5 i jeden slot OCP 3.0 x16.
Interfejsy sieciowe/FC/SAS Dwa interfejsy sieciowe 10/25GbE SFP28, cztery interfejsy sieciowe 1GbE Base-T
Dyski twarde Zainstalowane 5 x 1.92TB SSD SATA 6Gbps 512e 2.5in Hot-plug skonfigurowane fabrycznie w RAID 5.

Zainstalowane dwa dyski 480GB SSD SATA 6Gbps 512e 2.5in Hot-plug z możliwością konfiguracji RAID 1.
Kontroler RAID Główny kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Dodatkowy Kontorler typu BOSS.
Wbudowane porty min. port USB 2.0 oraz 2 x USB 3.1, port VGA,
System operacyjny Windows Server 2025 Standard na odpowiadającą ilość rdzeni procesora.
Video Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory Redundantne.
Zasilacze Min. dwa zasilacze Hot-Plug min. 800W Titanium każdy wraz z kablami zasilającymi o długości min. 2m.
Zamawiający wymaga min. 60 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
Serwer musi posiadać deklaracja CE.
Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.

Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2022, Microsoft Windows 2025 x64.
Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera.
Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet.

4.2.6.) Główny kod CPV: 48821000-9 - Serwery sieciowe

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 90 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Sposób oceny wg wzoru
Łączna ofertowa cena brutto waga 100%-100 pkt
CN Cena najtańszej oferty nie podlegającej odrzuceniu
C = ---------- x 100pkt
CB Cena badanej oferty
RAZEM 100% 100

Cena oferty (C) za realizację całego zamówienia według następującego wzoru:

C- liczba punktów otrzymanych przez ofertę badaną w kryterium „Cena oferty”
CN - najniższa cena spośród wszystkich ofert podlegających ocenie
CB - cena w ofercie badanej

1. Do oceny oferty w tym kryterium Zamawiający przyjmie cenę brutto oferty zaoferowaną przez
2. Wykonawcę w Formularzu oferty.
3. Dla kryteriów oceny ofert przyjmuje się, iż 1% wagi kryterium = 1 pkt i tak zostanie przeliczona liczba punktów.
4. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą liczbę punktów wyliczoną w zaokrągleniu do dwóch miejsc po przecinku.
5. Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Wyłącznie kryterium ceny

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 100

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 2

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 2- MACIERZ NAS – 1 sztuka
Nazwa komponentu Opis minimalnych wymagań technicznych
Typ Sieciowy serwer plików NAS
Obudowa Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.
Procesor Procesor klasy ARM, min. 4-rdzeniowy. Procesor osiągający w teście PassMark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 1100 pkt. według wyników publikowanych na stronie https://www.cpubenchmark.net/cpu-list/all

Pamięć RAM 2 GB UDIMM DDR4
Wewnętrzna pamięć masowa 3 dyski 8TB 3,5-calowe SATA 6 Gb/s,
Zainstalowane dyski muszą znajdować się na liście kompatybilnych urządzeń publikowanej przez producenta serwera NAS.
Możliwość dołożenia czwartego dysku.
Kompatybilność dysków 3,5-calowe wnęki:

3,5-calowe dyski twarde SATA
2,5-calowe dyski twarde SATA
2,5-calowe dyski SSD SATA
Interfejsy sieciowe Min. 2 x 2,5 Gigabit Ethernet (2,5G/1G/100M/10M), 2 x 10GbE SFP+
Złącza dodatkowe Min. 2 porty typu A USB 3.2,
Gniazdo M.2 Opcjonalne, poprzez kartę PCIe
Szyfrowanie AES 256bit
Zasilacz 250 W PSU, 100–240 V
Certyfikaty Producent serwera NAS musi posiadać certyfikat jakości według normy ISO 9001 na produkcję oferowanego asortymentu lub równoważny certyfikat jakości oraz certyfikat według normy ISO 14001 Systemu Zarządzania Środowiskowego lub równoważną normę zarządzania środowiskowego.
Gwarancja producenta 5 lat gwarancji Next Business Day Onsite na serwer.
5 lat gwarancji Next Business Day na dyski.
Dokumentacja użytkownika Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w formie elektronicznej.

4.2.6.) Główny kod CPV: 48823000-3 - Serwery plików

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 90 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: 1. Łączna ofertowa cena brutto- waga 60%- 60 pkt
Cena najtańszej oferty nie podlegającej odrzuceniu
C = ---------- x 60pkt
Cena badanej oferty
2. Termin dostawy- waga 40%- 40 pkt
1) Termin dostawy do 60 dni od podpisania umowy- 40 pkt;
2) Termin dostawy 61-90 dni od podpisania umowy-20 pkt.
3) Termin dostawy powyżej 90 dni -0 pkt.
RAZEM 100% 100 pkt

3 Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:
L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Termin dostawy”
4 Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
5 Ocena punktowa w kryterium „Termin dostawy”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
6 Ocena ofert w oparciu o kryterium „Termin dostawy” klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:
o Termin dostawy do 60 dni od podpisania umowy 40 pkt;
o Termin dostawy 61-90 dni od podpisania umowy 20 pkt;
o Termin dostawy powyżej 90 dni od podpisania umowy 0 pkt;
7 Ocena ofert w oparciu o kryterium „Termin dostawy” rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
8 Najkrótszy możliwy czas dostawy towaru to termin do 60 dni od podpisania umowy.
9 Najdłuższy możliwy czas dostawy towaru to termin powyżej 90 dni.
10 Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu dostawy zamawiający przyjmie do oceny maksymalny możliwy czas (czyli 90 dni), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
11 Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
12 W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
13 Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: Termin dostawy

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 3

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 3-ZAAWANSOWANY FIREWALL NOWEJ GENERACJI (NGFW) – 2 sztuki
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 5 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:
• Firewall.
• Ochrony w warstwie aplikacji.
• Protokołów routingu dynamicznego.
Parametry wydajnościowe:
1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 45 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 o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1.3 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 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.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
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. Możliwość filtrowania zapytań DNS 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).
Gwarancja oraz wsparcie:

System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.
Opisy do wymagań ogólnych:
1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

4.2.6.) Główny kod CPV: 32420000-3 - Urządzenia sieciowe

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 90 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: 1. Łączna ofertowa cena brutto- waga 60%- 60 pkt
Cena najtańszej oferty nie podlegającej odrzuceniu
C = ---------- x 60pkt
Cena badanej oferty
2. Termin dostawy- waga 40%- 40 pkt
1) Termin dostawy do 60 dni od podpisania umowy- 40 pkt;
2) Termin dostawy 61-90 dni od podpisania umowy-20 pkt.
3) Termin dostawy powyżej 90 dni -0 pkt.
RAZEM 100% 100 pkt

3 Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:
L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Termin dostawy”
4 Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
5 Ocena punktowa w kryterium „Termin dostawy”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
6 Ocena ofert w oparciu o kryterium „Termin dostawy” klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:
o Termin dostawy do 60 dni od podpisania umowy 40 pkt;
o Termin dostawy 61-90 dni od podpisania umowy 20 pkt;
o Termin dostawy powyżej 90 dni od podpisania umowy 0 pkt;
7 Ocena ofert w oparciu o kryterium „Termin dostawy” rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
8 Najkrótszy możliwy czas dostawy towaru to termin do 60 dni od podpisania umowy.
9 Najdłuższy możliwy czas dostawy towaru to termin powyżej 90 dni.
10 Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu dostawy zamawiający przyjmie do oceny maksymalny możliwy czas (czyli 90 dni), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
11 Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
12 W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
13 Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: Termin dostawy

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 4

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 4 –SCENTRALIZOWANY SYSTEM GROMADZENIA, ANALIZY I RAPORTOWANIA LOGÓW 1-sztuka
Wymagania Ogólne:
W ramach postępowania wymaganym jest dostarczenie systemu do zbierania, analizy i raportowania zdarzeń sieciowych i systemowych. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na Microsoft Hyper-V wersje 2019 i nowsze;
Interfejsy, Dysk:
1. System musi obsługiwać co najmniej 4 wirtualne interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.
Parametry wydajnościowe:
1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:
Logowanie:
1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
a. Listę najczęściej wykrywanych ataków.
b. Listę najbardziej aktywnych użytkowników.
c. Listę najczęściej wykorzystywanych aplikacji.
d. Listę najczęściej odwiedzanych stron www.
e. Listę krajów , do których nawiązywane są połączenia.
f. Listę najczęściej wykorzystywanych polityk Firewall.
g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
Raportowanie:
W zakresie raportowania system musi zapewniać:
1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
Korelacja logów:
W zakresie korelacji zdarzeń system musi zapewniać:
1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

• Malware.
• Aplikacje sieciowe.
• Email.
• IPS.
• Traffic.
• Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
Zarządzanie:
1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
Serwisy i licencje:
Wsparcie: System musi być objęty serwisem producenta przez okres min. 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Opisy do wymagań ogólnych:
1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

4.2.6.) Główny kod CPV: 48000000-8 - Pakiety oprogramowania i systemy informatyczne

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 90 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: 1. Łączna ofertowa cena brutto- waga 60%- 60 pkt
Cena najtańszej oferty nie podlegającej odrzuceniu
C = ---------- x 60pkt
Cena badanej oferty
2.Wydłużenie wsparcia oraz licencji aktualizacyjnej - waga 40%- 40 pkt
1. Wydłużenie wsparcia do 66 miesięcy - 40 pkt;
2. Wydłużenie wsparcia od 61 do 65 miesięcy -20 pkt.
3. Wydłużenie wsparcia do 60 miesięcy -0 pkt

RAZEM 100% 100 pkt
1) Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:
L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”

2) Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
3) Ocena punktowa w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
4) Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:
• Wydłużenie wsparcia do 66 miesięcy - 40 pkt;
• Wydłużenie wsparcia od 61 do 65 miesięcy -20 pkt.

• Wydłużenie wsparcia do 60 miesięcy -0 pkt
5) Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
6) Najkrótszy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 60 miesięcy.
7) Najdłuższy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 66 miesięcy.
8) Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu na wydłużenie wsparcia oraz licencji aktualizacyjnej zamawiający przyjmie do oceny minimalny możliwy czas (czyli 60 miesięcy), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
9) Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
10) W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
11) Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: Wydłużenie wsparcia oraz licencji aktualizacyjnej

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 5

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 5 - SYSTEM OCHRONY POCZTY – 1 SZTUKA
Wymagania ogólne
System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware-ową bez limitu licencyjnego na ilość chronionych kont użytkowników.
Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na Microsoft Hyper-V wersje 2019 i nowsze;
Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.
Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:
1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
Parametry fizyczne systemu antyspamowego:
1. System musi obsługiwać co najmniej 4 wirtualne interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.
Ogólne funkcje systemu ochrony poczty:
Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:
1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z

zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
Kontrola antywirusowa i ochrona przed malware:
W tym zakresie dostarczony system ochrony poczty musi zapewniać:
1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.
Kontrola antyspamowa:
System musi zapewniać poniższe funkcje i metody filtrowania spamu:
1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
Ochrona przed atakami na usługę poczty:
System musi zapewniać poniższe funkcje i metody filtrowania:
1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania:
W tym zakresie dostarczony system ochrony poczty musi zapewniać:
1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.

3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
Funkcje pracy w trybie wysokiej dostępności (HA):
System ochrony poczty musi zapewniać poniższe funkcje:
1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.
Aktualizacje sygnatur, dostęp do bazy spamu:
W tym zakresie dostarczony system ochrony poczty musi zapewniać:
1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie:
System ochrony poczty musi zapewniać poniższe funkcje:
1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
Certyfikaty:
Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:
1. VBSpam, VB100 rated, Common Criteria evaluation in process (NIAP), FIPS 140-3 Certified.
Serwisy i licencje:
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres min. 60 miesięcy.
Gwarancja oraz wsparcie:
System musi być objęty serwisem producenta przez okres min. 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

4.2.6.) Główny kod CPV: 48223000-7 - Pakiety oprogramowania do poczty elektronicznej

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 90 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: 1. Łączna ofertowa cena brutto- waga 60%- 60 pkt
Cena najtańszej oferty nie podlegającej odrzuceniu
C = ---------- x 60pkt
Cena badanej oferty
2.Wydłużenie wsparcia oraz licencji aktualizacyjnej - waga 40%- 40 pkt
1. Wydłużenie wsparcia do 66 miesięcy - 40 pkt;
2. Wydłużenie wsparcia od 61 do 65 miesięcy -20 pkt.
3. Wydłużenie wsparcia do 60 miesięcy -0 pkt

RAZEM 100% 100 pkt
1) Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:
L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”

2) Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
3) Ocena punktowa w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
4) Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:

• Wydłużenie wsparcia do 66 miesięcy - 40 pkt;
• Wydłużenie wsparcia od 61 do 65 miesięcy -20 pkt.
• Wydłużenie wsparcia do 60 miesięcy -0 pkt
5) Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej", rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
6) Najkrótszy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 60 miesięcy.
7) Najdłuższy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 66 miesięcy.
8) Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu na wydłużenie wsparcia oraz licencji aktualizacyjnej zamawiający przyjmie do oceny minimalny możliwy czas (czyli 60 miesięcy), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
9) Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
10) W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
11) Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: Wydłużenie wsparcia oraz licencji aktualizacyjnej

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 6

4.2.2.) Krótki opis przedmiotu zamówienia

CZEŚĆ 6- PROGRAM ANTYWIRUSOWY – 35 LICENCJI NA 3 LATA.
Centralne zarządzanie:
1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).
2. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim.
3. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID. 6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.
5. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.
6. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej:
• Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania.
• Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
• Buforowanie ruchu HTTPS.
7. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
8. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania.
9. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe.
10. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
11. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie.
13.Rozwiązanie musi udostępniać możliwość tagowania obiektów.
14. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

Ochrona stacji roboczych - Windows :

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia sumy kontrolnej (SHA1).
12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
13. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
• Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
• Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
• Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. Rozwiązanie musi udostępniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi udostępniać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji.
18. Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów:
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:
• Antywiruzs
• Zapora osobista.
• Sandbox.
• Antyspyware.
• Metody heurystyczne.
20.Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
21. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
22. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
a. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
• Skanowanie portów TCP oraz UDP,
• Wykrywanie duplikacji adresu IP,
• Atak zatruwania ARP,
• Nieprawidłowa długość pakietu TCP oraz UDP.
b. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
• RDP,
• SMB,
• My SQL, ➢ MS SQL.
c. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

4.2.6.) Główny kod CPV: 48761000-0 - Pakiety oprogramowania antywirusowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: 90 dni

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: 1. Łączna ofertowa cena brutto- waga 60%- 60 pkt
Cena najtańszej oferty nie podlegającej odrzuceniu
C = ---------- x 60pkt
Cena badanej oferty
2.Wydłużenie wsparcia oraz licencji aktualizacyjnej - waga 40%- 40 pkt
1) Wydłużenie wsparcia do 42 miesięcy - 40 pkt;
2) Wydłużenie wsparcia od 37 do 41 miesięcy -20 pkt.
3) Wydłużenie wsparcia do 36 miesięcy -0 pkt
24) Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:
L = C + P
gdzie:
L – całkowita liczba punktów,
C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto”,
P – punkty uzyskane w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”

3. Ocena punktowa w kryterium „Łączna cena ofertowa brutto” dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
4. Ocena punktowa w kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, dokonana zostanie na podstawie czasu wskazanego przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.
5. Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, klasyfikuje się następująco – na podstawie deklaracji w złożonej ofercie:
• Wydłużenie wsparcia do 42 miesięcy - 40 pkt;
• Wydłużenie wsparcia od 37 do 41 miesięcy -20 pkt.
• Wydłużenie wsparcia do 36 miesięcy -0 pkt
6. Ocena ofert w oparciu o kryterium „Wydłużenie wsparcia oraz licencji aktualizacyjnej”, rozpatrywana będzie na podstawie zadeklarowanego przez Wykonawcę w Formularzu Oferty j/w.
7. Najkrótszy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 36 miesięcy.
8. Najdłuższy możliwy termin na wydłużenie wsparcia oraz licencji aktualizacyjnej to termin do 42 miesięcy.
9. Jeżeli Wykonawca nie poda (nie wpisze) w Formularzu Oferty terminu na wydłużenie wsparcia oraz licencji aktualizacyjnej zamawiający przyjmie do oceny minimalny możliwy czas (czyli 36 miesięcy), a w przypadku wyboru oferty Wykonawcy czas ten zostanie uwzględniony w umowie.
10. Zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji warunków zamówienia.
11. W toku dokonywania oceny złożonych ofert Zamawiający, na podstawie art. 223 ust. 1 Pzp, może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń.
12. Zamawiający odrzuci ofertę, jeżeli zaistnieją przypadki określone w art. 226 Pzp.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: Wydłużenie wsparcia oraz licencji aktualizacyjnej

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

SEKCJA V - KWALIFIKACJA WYKONAWCÓW

5.1.) Zamawiający przewiduje fakultatywne podstawy wykluczenia: Tak

5.2.) Fakultatywne podstawy wykluczenia:

Art. 109 ust. 1 pkt 4

5.3.) Warunki udziału w postępowaniu: Tak

5.4.) Nazwa i opis warunków udziału w postępowaniu.
1. spełniają warunki udziału w postępowaniu dotyczące:
a) zdolności do występowania w obrocie gospodarczym:
Zamawiający nie określa warunku w tym zakresie.

b) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:
Zamawiający nie określa warunku w tym zakresie.

c) sytuacji finansowej lub ekonomicznej:
Zamawiający nie określa warunku w tym zakresie.

d) zdolności technicznej lub zawodowej:

Wykonawca spełni warunek, jeżeli w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – wykonał co najmniej 1 dostawę (zawartą umowę na dostawę), oraz załączy na wezwanie dowody określające, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane co najmniej 12 miesięcy.

Dla części nr 1 i 5:

polegające na dostawie sprzętu informatycznego np. zestawów komputerowych, sprzętu multimedialnego, urządzeń wielofunkcyjnych, sprzętu i osprzętu informatycznego oraz oprogramowania o wartości co najmniej 50 000,00 zł brutto.

Dla części nr 2, 3, 4, 6:
polegające na dostawie sprzętu informatycznego np. zestawów komputerowych, sprzętu multimedialnego, urządzeń wielofunkcyjnych, sprzętu i osprzętu informatycznego oraz oprogramowania o wartości co najmniej 17 000,00 zł brutto.

5.5.) Zamawiający wymaga złożenia oświadczenia, o którym mowa w art.125 ust. 1 ustawy: Tak

5.6.) Wykaz podmiotowych środków dowodowych na potwierdzenie niepodlegania wykluczeniu: 1. Oświadczenie o braku podstaw do wykluczenia, sporządzone zgodne ze wzorem stanowiącym załącznik nr 2 do SWZ.
2. Oświadczenia o aktualności informacji podanych w oświadczeniu z art. 125 ust. 1 PZP załącznik nr 3 do SWZ.
W przypadku wspólnego ubiegania się o zamówienie przez wielu Wykonawców, oświadczenie składa każdy z Wykonawców, oświadczenia te potwierdzają brak podstaw wykluczenia.
3. W przypadku gdy oferta nie została podpisana przez osobę uprawnioną do reprezentacji Wykonawcy określoną w odpowiednim rejestrze lub innym dokumencie właściwym dla danej formy organizacyjnej Wykonawcy, do oferty należy dołączyć pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy w formie elektronicznej.
4. Załącznik nr 4 do SWZ. Oświadczenie o udostępnieniu zasobów (podpisuje podmiot udostępniający zasoby). Dokument należy dołączyć do oferty - jeżeli ma zastosowanie.
5. Załącznik nr 5 do SWZ - Oświadczenie Wykonawców składający ofertę wspólnie (gdy ma zastosowanie).
6. Oświadczenia, o których mowa wyżej stanowią dowód potwierdzający brak podstaw wykluczenia na dzień składania ofert. Oświadczenie te składa się, pod rygorem nieważności, w formie elektronicznej (tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
7. Jeżeli złożone przez wykonawcę oświadczenie, o którym mowa w art. 125 ust. 1 PZP, lub podmiotowe środki dowodowe budzą wątpliwości Zamawiającego, może on zwrócić się bezpośrednio do podmiotu, który jest w posiadaniu informacji lub dokumentów istotnych w tym zakresie dla oceny spełniania przez Wykonawcę warunków udziału w postępowaniu lub braku podstaw wykluczenia, o przedstawienie takich informacji lub dokumentów.
8. W przypadku oferty Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum, spółka cywilna):
• w formularzu oferty należy wskazać firmy (nazwy) wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
• oferta musi być podpisana w taki sposób, by wiązała prawnie wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Osoba podpisująca ofertę musi posiadać umocowanie prawne do reprezentacji. Umocowanie musi wynikać z treści pełnomocnictwa załączonego do oferty – treść pełnomocnictwa powinna dokładnie określać zakres umocowania;
• wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia będą ponosić odpowiedzialność solidarną za wykonanie umowy.
9. Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
10. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 PZP, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
11. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 PZP, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem

elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych jeśli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005r. informatyzacji działalności podmiotów realizujących zadnia publiczne (tekst jedn. Dz. U. z 2023 r. poz. 57 z późn. zm.), o ile Wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 PZP, dane umożliwiające dostęp do tych środków

5.7.) Wykaz podmiotowych środków dowodowych na potwierdzenie spełniania warunków udziału w postępowaniu:
Wykonawca spełni warunek, jeżeli w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – wykonał co najmniej 1 dostawę (zawartą umowę na dostawę), oraz załączy na wezwanie dowody określające, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane co najmniej 12 miesięcy:
Dla części nr 1 i 5:

polegające na dostawie sprzętu informatycznego np. zestawów komputerowych, sprzętu multimedialnego, urządzeń wielofunkcyjnych, sprzętu i osprzętu informatycznego oraz oprogramowania o wartości co najmniej 50 000,00 zł brutto.

Dla części nr 2, 3, 4, 6:
polegające na dostawie sprzętu informatycznego np. zestawów komputerowych, sprzętu multimedialnego, urządzeń wielofunkcyjnych, sprzętu i osprzętu informatycznego oraz oprogramowania o wartości co najmniej 17 000,00 zł brutto.

5.11.) Wykaz innych wymaganych oświadczeń lub dokumentów:
Na wezwanie Zamawiającego:
1. Oświadczenie o spełnieniu norm środowiskowych - dotyczy części 1 (pierwszej) przedmiotu zamówienia.
2. Oświadczenie potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta- dotyczy części 1 (pierwszej) przedmiotu zamówienia.
3. Oświadczenie potwierdzające spełnienie wymagań Karty Zarządzania- dotyczy części 1 (pierwszej) przedmiotu zamówienia.
4. Oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta - dotyczy części 1 (pierwszej) przedmiotu zamówienia.

SEKCJA VI - WARUNKI ZAMÓWIENIA

6.1.) Zamawiający wymaga albo dopuszcza oferty wariantowe: Nie

6.3.) Zamawiający przewiduje aukcję elektroniczną: Nie

6.4.) Zamawiający wymaga wadium: Nie

6.5.) Zamawiający wymaga zabezpieczenia należytego wykonania umowy: Nie

6.6.) Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:
W przypadku oferty Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum, spółka cywilna):
• w formularzu oferty należy wskazać firmy (nazwy) wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
• oferta musi być podpisana w taki sposób, by wiązała prawnie wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Osoba podpisująca ofertę musi posiadać umocowanie prawne do reprezentacji. Umocowanie musi wynikać z treści pełnomocnictwa załączonego do oferty – treść pełnomocnictwa powinna dokładnie określać zakres umocowania;
• wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia będą ponosić odpowiedzialność solidarną za wykonanie umowy.

6.7.) Zamawiający przewiduje unieważnienie postępowania, jeśli środki publiczne, które zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia nie zostały przyznane: Nie

SEKCJA VII - PROJEKTOWANE POSTANOWIENIA UMOWY

7.1.) Zamawiający przewiduje udzielenia zaliczek: Nie

7.3.) Zamawiający przewiduje zmiany umowy: Nie

7.5.) Zamawiający uwzględnił aspekty społeczne, środowiskowe, innowacyjne lub etykiety związane z realizacją zamówienia: Nie

SEKCJA VIII – PROCEDURA

8.1.) Termin składania ofert: 2026-05-18 09:00

8.2.) Miejsce składania ofert: Ofertę należy złożyć za pośrednictwem Platformy e-Zamówienia: https://ezamowienia.gov.pl

8.3.) Termin otwarcia ofert: 2026-05-18 10:00

8.4.) Termin związania ofertą: 30 dni