



Cyberbezpieczny Samorząd

„Podniesienie poziomu cyberbezpieczeństwa Starostwa Powiatowego w Sępólnie Krajeńskim”



Nr sprawy: AB.272.15.2025

Specyfikacja Warunków Zamówienia

**Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego
w ramach projektu Cyberbezpieczny Powiat**

Zatwierdził:

Jarosław Tadyh
Starosta Sępoleński

Sępólno Kraj., dn. 9 grudnia 2025 r.

CZĘŚĆ I. NAZWA I ADRES ZAMAWIAJĄCEGO, ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA.

1. **Powiat Sępoleński reprezentowany przez Starostę Sępoleńskiego**
2. Adres: 89-400 Sępólno Kraj., ul. Kościuszki 11
3. Telefon: **52 388 13 00** Fax: **52 388 13 03**
4. e-mail: sekretariat@powiat-sepolno.pl
5. Adres internetowy: www.powiat-sepolno.pl
6. Numer NIP: **561 13 27 106** Numer REGON: **092361522**
7. Adres strony internetowej prowadzonego postępowania:
<https://ezamowienia.gov.pl/mp-client/tenders/ocds-148610-270c2682-1494-4df1-843a-053805913df9>
8. Identyfikator (ID) postępowania na Platformie e-Zamówienia:
ocds-148610-270c2682-1494-4df1-843a-053805913df9
9. ID techniczne: **8719**

CZĘŚĆ II. TRYB UDZIELENIA ZAMÓWIENIA, INFORMACJA, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ OFERTY Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI

1. Postępowanie prowadzone jest w trybie podstawowym bez możliwości negocjacji na podstawie art.275 pkt.1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz.1320 z późn. zm.), zwanej dalej „*ustawą*”, oraz zgodnie z wymogami określonymi w niniejszej Specyfikacji Warunków Zamówienia.
2. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
3. Objasnienia używanych terminów:
SWZ – specyfikacja warunków zamówienia
Ustawa PZP – ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2024 r. poz.1320 z późn. zm.).

CZĘŚĆ III . OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **„Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat”**.

Nazwy i kody zamówienia według Wspólnego Słownika Zamówień(CPV):

48821000-9 Serwery sieciowe

32420000-3 Urządzenia sieciowe

Zamówienie jest realizowane w ramach grantu w projekcie grantowym **„Cyberbezpieczny Samorząd”** współfinansowanym przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: *Zaawansowane usługi cyfrowe*, Działanie 2.2. –

Wzmocnienie krajowego systemu cyberbezpieczeństwa, na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1769/ FERC.02.02-CS.01-001/23/2024.

2. Przedmiot zamówienia obejmuje **2 części**, dla których Zamawiający dopuszcza możliwość składania ofert częściowych, z zastrzeżeniem, iż oferta w każdej z części winna być pełna i powinna spełniać szczegółowe wymagania określone w SWZ. Wykonawca może złożyć ofertę na każdą dowolnie wybraną przez siebie część. Zamawiający nie ogranicza liczby części, na które może złożyć ofertę jeden Wykonawca.

3. Opis przedmiotu zamówienia:

1) CZĘŚĆ 1 - Urządzenie do backupu

(serwer, macierz i oprogramowanie do wykonywania kopii zapasowej)

- a) Oferowane serwery i macierz muszą pochodzić od jednego producenta, posiadać wszystkie wymagane funkcje i być fabrycznie nowe, w szczególności nieużywane, nieregenerowane, nienaprawiane.
- b) Oferowane serwery i macierz muszą być wyprodukowane nie wcześniej (nie mogą być starsze) niż 6 miesięcy przed datą dostawy.
- c) Zamawiający dopuszcza zastosowanie sprzętu i oprogramowania równoważnego, poprzez który należy rozumieć sprzęt i oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co sprzęt i oprogramowanie określone w opisie przedmiotu zamówienia.
- d) Oferowane serwery i macierz muszą współpracować w ramach klastra niezawodnościowego, który w przypadku awarii jednego z węzłów zapewni automatyczną migrację usług (maszyn wirtualnych) z uszkodzonego węzła na węzeł działający. Musi także oferować mechanizm wstrzymania pracy jednego węzła (bez przerywania ciągłości usług na nim działających) w celu przeprowadzenia aktualizacji, naprawy lub innych prac serwisowych.
- e) Oferowane serwery i macierz muszą posiadać pełne wsparcie producenta sprzętu oraz oprogramowania wirtualizacyjnego (rozwiązanie certyfikowane) do pracy w klastrze niezawodnościowym.

**Serwer przeznaczony do wykonywania kopii zapasowych oraz do pracy w klastrze
niezawodnościowym – 1 sztuka**

Obudowa

- Typu RACK, wysokość nie więcej niż 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Obudowa umożliwiająca instalację 24 dysków twardych Hot-Plug;
- Zainstalowane 2 szt. dysków SSD NVMe 960GB HOT-PLUG skonfigurowane w bios serwera w RAID-1;

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Moduł TPM 2.0;
- 3 złącza PCI Express w tym minimum 1 złącze x16;
- Opcjonalnie możliwość uzyskania 10 slotów PCIe;
- 32 gniazda pamięci RAM;
- Obsługa 8 TB pamięci operacyjnej RAM DDR5;
- Wsparcie dla technologii:
- Bounded Fault;
- SDDC;
- ECC;
- Memory Mirroring;
- ADDDC;
- Wewnętrzny slot na kartę Micro SD

Procesory

- Dwa procesory 8-rdzeniowe, taktowanie bazowe 3,2 GHz, architektura x86_64;
- Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 274 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org/> dla oferowanego serwera.

Pamięć RAM

- 512GB pamięci RAM;
- DDR5 Registered 5600MT/s;
- Obsadzone w trybie maksymalnej wydajności (maksymalnie połowa zajętych gniazd);

Kontrolery LAN

- Interfejsy LAN, nie zajmujące slotów PCI Express (OCP):
- 4x 1Gbit Base-T;
- Możliwość uzyskania 2 interfejsów 100Gbit QSFP56 bez konieczności instalacji kart w slotach PCIe;
- 1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB;
- Dodatkowe interfejsy LAN:
- 2x 25Gbit SFP28 obsadzone wkładkami 10/25G MMF LC;
- 2 x 10Gbit Ethernet – na karcie PCIe,

Kontrolery I/O

- Kontroler FC 2x 32Gb MMF LC obsadzony wkładkami FC 32GB, oraz z dołączonym okablowaniem 2 x FC-Cable OM4, MMF, 5m, LC/LC

Porty

- Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera;
- 3 porty USB dostępne z tyłu serwera w tym dwa w wersji USB 3.2;
- 1 port USB 3.2 wewnętrzny;
- 2 porty USB na panelu przednim w tym jeden w wersji USB 3.2;
- Jeden z frontowych portów USB musi posiadać możliwość zarządzania serwerem;
- Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera;
- Opcjonalny port serial;
- Ilość dostępnych złączy USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1100W;
- Redundantne dwuwirnikowe wentylatory hotplug dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni celsjusza;

Bezpieczeństwo

- Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji;
- Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej;
- Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem;
- Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem;
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania;
- Możliwość ustawienia hasła włączania serwera;
- Możliwość ustawienia hasła administratora;
- Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID;

Zarządzanie

- Wymaga się aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
- Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych;
- Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.
- Funkcjonalność kontrolera zdalnego zarządzania:
- Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)

- Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja
- Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
- Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.
- Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3
- Update systemowego firmware
- Monitoring i możliwość ograniczenia poboru prądu
- Zdalne włączanie/wyłączanie/restart
- Zapis video zdalnych sesji
- Podmontowanie lokalnych mediów z wykorzystaniem Java client
- Przekierowanie konsoli szeregowej przez IPMI
- Zrzut ekranu w momencie zawieszenia systemu
- Możliwość przejęcia zdalnego ekranu
- Możliwość zdalnej instalacji systemu operacyjnego
- Alerty Syslog
- Przekierowanie konsoli szeregowej przez SSH
- Wsparcie dla dynamic DNS
- Wyświetlanie danych aktualnych i historycznych dla zużycia energii oraz temperatury serwera
- Wirtualna konsola z dostępem do myszy, klawiatury;
- Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy ActiveX (musi działać w oparciu o HTML5)
- Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
- Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
- wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API
- Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiegokolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
- Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.
- Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.
- Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.
- Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
- Oprogramowanie producenta serwera służące do zarządzania, spełniające poniższe wymagania:
- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- Integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym
- Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP
- Szczegółowy opis wykrytych systemów oraz ich komponentów

- Możliwość eksportu danych min do formatu CSV
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK
- Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych
- Możliwość przejęcia zdalnego pulpitu
- Możliwość zamontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta
- Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)
- Automatyczna polityka aktualizacji „Najnowsze dostępne”
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym
- Możliwość automatycznego generowania i zgłaszania incydentów awariibezpośrednio do centrum serwisowego producenta serwerów
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI
- Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:
 - wykonać zautomatyzowaną aktualizację firmware serwerów w clustrze Vmware do zdefiniowanej polityki poziomu mikrokodów
 - wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji
 - z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
 - inwentaryzacja komponentów w serwerze i ich mikrokodów
 - historia min 24h poboru mocy i temperatury serwera
 - zbieranie danych diagnostycznych serwera do paczki
- Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin:

- wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze do zdefiniowanej polityki poziomu mikrokodów
- z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
- aktualizacja sterowników systemowych Windows
- inwentaryzacja komponentów w serwerze i ich mikrokodów
- historia min 24h poboru mocy i temperatury serwera
- zbieranie danych diagnostycznych serwera do paczki
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Certyfikowane systemy operacyjne

- Microsoft Windows Server 2025, 2022, 2019;
- VMWare ESXi 8.0, 7.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9.x, 8.x;
- Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS,
- Microsoft Windows 11
- Oracle Linux 8.x, 9.x;
- Xen Server 8, Xen Hypervisor 8.2

Gwarancja

- 5 lat gwarancji producenta serwera w trybie on-site z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem zakończenia naprawy 24h od skutecznego zgłoszenia awarii do organizacji serwisowej producenta. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
- Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

System operacyjny

- Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Server Standard 2025 na 32 rdzenie lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności. Oferowany system musi mieć możliwość zainstalowania co najmniej 1 wersji wstecz (tj. Windows Server 2022 – należy dostarczyć licencję oraz nośnik).
- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard 2025:
 - Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i czterech wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji;
 - Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.

- Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – *wymagane oświadczenie wykonawcy lub producenta przed podpisaniem umowy*;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – *wymagane oświadczenie wykonawcy lub producenta przed podpisaniem umowy*;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

Macierz dyskowa przeznaczona do pracy jako storage do kopii zapasowej oraz do pracy w klastrze niezawodnościowym – 1 sztuka

Ogólne

- System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii.
- Oferowana macierz musi obsługiwać min. 264 dyski wykonanych w technologii hot-plug.
- Macierz musi posiadać 4 porty SAS 12 Gb/s do podłączenia dodatkowych półek dyskowych.

Pojemność macierzy:

- 5 szt. dysków 3,8TB SSD-SAS
- 9 szt. dysków 2,4TB SAS 10k RPM

Kontrolery

- Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami.
- Każdy z kontrolerów macierzy musi posiadać po minimum 32GB pamięci podręcznej Cache.
- W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci kontrolera muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.
- Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 4TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD.
- Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.
- Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.
- Każdy z kontrolerów RAID powinien posiadać dedykowany interfejs RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
- Oferowana macierz musi mieć wyprowadzone 2 porty iSCSI 25Gbps oraz 4 porty FC 32GBps (obsadzone modułami 32G LC MMF) do dołączenia serwerów bezpośrednio lub do sieci SAN na każdy kontroler RAID.
- Macierz musi umożliwiać wymianę co najmniej połowy zainstalowanych portów do transmisji danych na porty:
 - SAS 12 Gbps

- iSCSI 10Gbps Base-T

Poziomy RAID

- Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:
 - Raid-1
 - Raid-10
 - Raid-5
 - Raid-6
- Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.
- Macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.
- Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi.

Dyski

- Oferowana macierz musi wspierać dyski hot-plug:
 - dyski elektroniczne SSD
 - mechaniczne HDD z interfejsem SAS12Gb/s
 - dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,
- Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD zainstalowanych w dowolnym module rozwiązania.
- Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug.
- Macierz musi obsługiwać 120 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami.
- Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD.
- Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy).
- W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego, wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess).
- Macierz musi pozwalać na zaszyfrowanie danych na dedykowanych do tego dyskach kluczem AES256-bit zgodnie z wytycznymi Information Technology Laboratory przy National Institute of Standards and Technology (NIST).
- Macierz musi posiadać możliwość skasowania wszystkich danych z dysku FDE celem

bezpiecznego ponownego użycia w innym środowisku (Secure Erase).

Opcje programowe

- Macierz musi być wyposażona w system kopii migawkowych umożliwiający wykonanie 128 kopii migawkowych z opcją rozbudowy do 512.
- Macierz musi umożliwiać zdefiniowanie min. 1984 woluminy (LUN).
- Macierz powinna umożliwiać połączenie logiczne z minimum 500 serwerami.
- Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów.
- 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 systemów operacyjnych:
 - Microsoft Windows Server 2019, 2022, 2025
 - SuSE Linux Enterprise Server 15, 12
 - Red Hat Linux Enterprise Server 9, 8
 - Vmware vSphere 7, 8;
- Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.
- Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie asynchronicznym i synchronicznym, bez konieczności stosowania zewnętrznych urządzeń konwersji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych.
- Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych).
- Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin.

Zarządzanie

- Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej.
- Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.
- Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (minimum Microsoft Edge, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.

- Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modulem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.
- Wraz z systemem musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:
 - wydajności i opóźnień na wolumenach
 - wydajności I/Ops, MB/s
 - trafności w cache
- 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 Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter
- Macierz musi posiadać wsparcie dla VMware vSphere Storage APIs Array Integration (VAAI)

Gwarancja i serwis

- Całe rozwiązanie musi być objęte minimum 60 miesięcznym okresem gwarancji z naprawą w miejscu instalacji urządzenia i z gwarantowanym czasem zakończenia naprawy 24h od skutecznego zgłoszenia awarii do organizacji serwisowej producenta macierzy.
- Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej.
- Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia.
- Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych.
- Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia.
- Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje.

Oprogramowanie do wykonywania kopii zapasowych:

- Licencja wieczysta dla minimum 15 maszyn wirtualnych ze wsparciem i poprawkami do 30.06.2026 r.
- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x, 8.x oraz Microsoft Hyper-V 2016, 2019, 2022 oraz 2025.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez Vmware vCenter oraz pojedynczymi hostami
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual

Machine Manager, klastrami hostów oraz pojedynczymi hostami.

- Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej oraz nie posiadać ograniczeń licencyjnych co do ilości przechowywanych danych
- Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności
- 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 lub serwisami online. 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 zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
- Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP.
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota (migawki).
- 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 wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- 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 wspierać natywnie kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
- Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
- Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu.
- 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
- Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
- Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
- Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
- Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
 - Linux * ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
 - Mac * HFS, HFS+
 - 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
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL Server włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia
- Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
- Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych.
- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsolę vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016, 2019, 2022, 2025
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

Serwer przeznaczony do analizy logów oraz do pracy w klastrze niezawodnościowym

– 1 sztuka

Obudowa

- Typu RACK, wysokość nie więcej niż 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Obudowa umożliwiająca instalację 24 dysków twardych Hot-Plug;
- Zainstalowane 2 szt. dysków SSD NVMe 960GB HOT-PLUG skonfigurowane w bios serwera w RAID-1;

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Moduł TPM 2.0;
- 3 złącza PCI Express w tym minimum 1 złącze x16;
- Opcjonalnie możliwość uzyskania 10 slotów PCIe;
- 32 gniazda pamięci RAM;
- Obsługa 8 TB pamięci operacyjnej RAM DDR5;
- Wsparcie dla technologii:
- Bounded Fault;
- SDDC;
- ECC;
- Memory Mirroring;
- ADDDC;
- Wewnętrzny slot na kartę Micro SD

Procesory

- Dwa procesory 8-rdzeniowe, taktowanie bazowe 3,2 GHz, architektura x86_64;
- Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 274 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org/> dla oferowanego serwera.

Pamięć RAM

- 512GB pamięci RAM;
- DDR5 Registered 5600MT/s;
- Obsadzone w trybie maksymalnej wydajności (maksymalnie połowa zajętych gniazd);

Kontrolery LAN

- Interfejsy LAN, nie zajmujące slotów PCI Express (OCP):
- 4x 1Gbit Base-T;
- Możliwość uzyskania 2 interfejsów 100Gbit QSFP56 bez konieczności instalacji kart w slotach PCIe;
- 1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB;
- Dodatkowe interfejsy LAN:
- 2x 25Gbit SFP28 obsadzone wkładkami 10/25G MMF LC;
- 2 x 10Gbit Ethernet – na karcie PCIe,

Kontrolery I/O

- Kontroler FC 2x 32Gb MMF LC obsadzony wkładkami FC 32GB, oraz z dołączonym

okablowaniem 2 x FC-Cable OM4, MMF, 5m, LC/LC

Porty

- Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera;
- 3 porty USB dostępne z tyłu serwera w tym dwa w wersji USB 3.2;
- 1 port USB 3.2 wewnętrzny;
- 2 porty USB na panelu przednim w tym jeden w wersji USB 3.2;
- Jeden z frontowych portów USB musi posiadać możliwość zarządzania serwerem;
- Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera;
- Opcjonalny port serial;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1100W;
- Redundantne dwuwirnikowe wentylatory hotplug dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni celsjusza;

Bezpieczeństwo

- Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji;
- Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej;
- Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem;
- Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem;
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania;
- Możliwość ustawienia hasła włączania serwera;
- Możliwość ustawienia hasła administratora;
- Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID;

Zarządzanie

- Wymaga się aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
- Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów

takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych;

- Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.
- Funkcjonalność kontrolera zdalnego zarządzania:
- Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)
- Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja
- Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
- Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/installacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.
- Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3
- Update systemowego firmware
- Monitoring i możliwość ograniczenia poboru prądu
- Zdalne włączanie/wyłączanie/restart
- Zapis video zdalnych sesji
- Podmontowanie lokalnych mediów z wykorzystaniem Java client
- Przekierowanie konsoli szeregowej przez IPMI
- Zrzut ekranu w momencie zawieszenia systemu
- Możliwość przejęcia zdalnego ekranu
- Możliwość zdalnej instalacji systemu operacyjnego
- Alerty Syslog
- Przekierowanie konsoli szeregowej przez SSH
- Wsparcie dla dynamic DNS
- Wyświetlanie danych aktualnych i historycznych dla zużycia energii oraz temperatury serwera
- Wirtualna konsola z dostępem do myszy, klawiatury;
- Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy ActiveX (musi działać w oparciu o HTML5)
- Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
- Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
- wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMi v1.5, REST API
- Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
- Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera

zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.

- Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.
- Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.
- Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
- Oprogramowanie producenta serwera służące do zarządzania, spełniające poniższe wymagania:
 - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
 - Integracja z Active Directory
 - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym
 - Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP
 - Szczegółowy opis wykrytych systemów oraz ich komponentów
 - Możliwość eksportu danych min do formatu CSV
 - Grupowanie urządzeń w oparciu o kryteria użytkownika
 - Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK
 - Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS
 - Szybki podgląd stanu środowiska
 - Podsumowanie stanu dla każdego urządzenia
 - Szczegółowy status urządzenia/elementu/komponentu
 - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
 - Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych
 - Możliwość przejęcia zdalnego pulpitu
 - Możliwość zamontowania wirtualnego napędu
 - Kreator umożliwiający dostosowanie akcji dla wybranych alertów
 - Przesyłanie alertów „as-is” do innych konsol firm trzecich
 - Możliwość definiowania ról administratorów
 - Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
 - Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta
 - Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)
 - Automatyczna polityka aktualizacji „Najnowsze dostępne”
 - Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym
 - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów

- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.
- Wdrażanie serwerów, rozwiązań modułowych oraz przełączników sieciowych w oparciu o profile
- Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI
- Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:
 - wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów
 - wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji
 - z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
 - inwentaryzacja komponentów w serwerze i ich mikrokodów
 - historia min 24h poboru mocy i temperatury serwera
 - zbieranie danych diagnostycznych serwera do paczki
- Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin:
 - wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze do zdefiniowanej polityki poziomu mikrokodów
 - z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
 - aktualizacja sterowników systemowych Windows
 - inwentaryzacja komponentów w serwerze i ich mikrokodów
 - historia min 24h poboru mocy i temperatury serwera
 - zbieranie danych diagnostycznych serwera do paczki
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Certyfikowane systemy operacyjne

- Microsoft Windows Server 2025, 2022, 2019;
- VMWare ESXi 8.0, 7.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9.x, 8.x;
- Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS,
- Microsoft Windows 11
- Oracle Linux 8.x, 9.x;
- Xen Server 8, Xen Hypervisor 8.2

Gwarancja

- 5 lat gwarancji producenta serwera w trybie on-site z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem zakończenia naprawy 24h od skutecznego zgłoszenia awarii do organizacji serwisowej producenta. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
- Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

System operacyjny

- Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Server Standard 2025 na 32 rdzenie lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności. Oferowany system musi mieć możliwość zainstalowania co najmniej 1 wersji wstecz (tj. Windows Server 2022 – należy dostarczyć licencję oraz nośnik).
- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard 2025:
 - Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i czterech wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji;
 - Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
 - Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
 - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 - Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 - Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 - Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
 - Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

- Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – *wymagane oświadczenie wykonawcy lub producenta przed podpisaniem umowy*;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – *wymagane oświadczenie wykonawcy lub producenta przed podpisaniem umowy*;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

W ramach dostawy wdrożenie oprogramowania do monitorowania logów systemowych (1 szt.).

Wykonawca jest zobowiązany zainstalować oprogramowanie do monitorowania logów systemowych na tym serwerze.

Minimalne parametry funkcjonalne oprogramowania do agregacji logów:

- System musi umożliwiać zbieranie logów z szerokiego spektrum źródeł, takich jak systemy operacyjne (Linux, Windows, macOS), aplikacje, urządzenia sieciowe, bazy danych, serwery webowe, oraz platformy chmurowe (np. AWS, Azure, Google Cloud).
- System musi wspierać zbieranie logów w różnych formatach, w tym min. Syslog oraz plain text zapewniając możliwość monitorowania standardowych i niestandardowych źródeł danych.
- System musi centralizować logi z wszystkich podłączonych źródeł umożliwiając ich łatwe zarządzanie i analizę w jednym miejscu.
- System musi oferować zaawansowane funkcje filtracji logów.
- System musi posiadać funkcję normalizacji logów pochodzących z różnych źródeł umożliwiając standaryzację danych i ich późniejszą korelację.
- System musi posiadać mechanizm korelacji zdarzeń, który umożliwia łączenie i analizowanie zdarzeń pochodzących z różnych źródeł w celu wykrywania bardziej złożonych zagrożeń.

- System musi wspierać tworzenie i zarządzanie regułami korelacji, które mogą być dostosowywane do specyficznych potrzeb organizacji, a także grupowane według źródła logów, rodzaju zagrożenia lub poziomu krytyczności.
- System musi umożliwiać hierarchizację reguł umożliwiając tworzenie bardziej zaawansowanych strategii wykrywania zagrożeń.
- System musi posiadać silniki detekcji zagrożeń, które analizują logi w czasie rzeczywistym, identyfikując złośliwe działania, próby włamań, naruszenia polityk bezpieczeństwa oraz inne anomalie.
- System musi wspierać wykrywanie zagrożeń opartych zarówno na sygnaturach, jak i na anomaliach umożliwiając szybkie reagowanie na nowe i nieznane wcześniej zagrożenia.
- System musi posiadać funkcję wykrywania specyficznych rodzajów ataków, takich jak brute force, ataki DDoS, próby eskalacji uprawnień, ataki typu SQL injection, czy próby przejęcia kont użytkowników.
- System musi umożliwiać dynamiczne przypisywanie poziomów krytyczności do wykrytych zdarzeń pozwalając na priorytetyzację incydentów bezpieczeństwa.
- System musi generować alarmy w czasie rzeczywistym, z możliwością ich wysyłania przez e-mail, webhooki, do systemów SIEM lub innych systemów zarządzania incydentami.
- System musi oferować możliwość korelacji i łączenia alarmów zapewniając pełny kontekst zdarzenia i redukcji liczbę fałszywych alarmów.
- System musi umożliwiać archiwizację wszystkich zebranych logów z możliwością ich przeszukiwania w celu przeprowadzania analizy historycznej oraz audytów po incydencie.
- System musi posiadać funkcję generowania raportów zgodności z regulacjami, takimi jak PCI DSS, GDPR oraz inne z możliwością dostosowywania tych raportów do specyficznych wymagań Zamawiającego.
- System musi oferować możliwość tworzenia niestandardowych raportów, które mogą zawierać szczegółowe zestawienia zdarzeń, analizę trendów oraz ocenę skuteczności polityk bezpieczeństwa.
- System musi udostępniać API RESTful pozwalające na integrację z zewnętrznymi systemami oraz automatyzację procesów związanych z analizą logów i zarządzaniem incydentami.
- System musi oferować integrację z zewnętrznymi bazami danych zagrożeń, takimi jak VirusTotal, w celu automatycznego sprawdzania logów związanych z plikami pod kątem znanych zagrożeń.
- System musi wspierać integrację z honeypotami pozwalając na wykrywanie i analizowanie prób ataków na pułapki umożliwiając lepsze zrozumienie działań atakujących.
- System musi posiadać funkcję geolokalizacji IP w analizowanych logach umożliwiając identyfikowanie podejrzanych połączeń z nieautoryzowanych lokalizacji.
- System musi oferować interaktywne dashboardy do monitorowania logów w czasie rzeczywistym z możliwością ich dostosowania do specyficznych potrzeb operacyjnych Zamawiającego.
- System musi umożliwiać tworzenie spersonalizowanych widoków i filtrów, które pozwolą na szybką identyfikację incydentów i anomalii dostosowanych do potrzeb administratorów.
- System musi zapewniać szyfrowanie komunikacji między serwerem a agentami tak, aby

zabezpieczyć dane przed nieautoryzowanym dostępem i zapewnić integralność przesyłanych logów.

- System musi posiadać mechanizmy autoryzacji i autentykacji użytkowników umożliwiając kontrolę dostępu do danych, konfiguracji oraz interfejsów zarządzających.
- Zamawiający oczekuje dostawy oprogramowania na licencji typu „open source”.

Wdrożenie oprogramowania do agregacji logów – minimalny zakres prac Wykonawcy:

- Wdrożenie powinno uwzględniać wszystkie funkcjonalności oprogramowania od zbierania logów po ich analizę, korelację i generowanie raportów.
- Wdrożenie powinno odbyć się na rzecz i uwzględniając infrastrukturę Starostwa Powiatowego w Sępólnie Krajeńskim.
- W ramach wdrożenia należy przeprowadzić analizę wstępną, w ramach której: Należy przeprowadzić ocenę infrastruktury: Dokładnie zidentyfikować wszystkie urządzenia w sieci, w tym serwery, przełączniki, komputery, drukarki, routery, firewalles i inne urządzenia sieciowe. Wskazać, które z nich generują logi, które będą zbierane i analizowane przez oprogramowanie.
- Należy określić wymagania: Zidentyfikować specyficzne potrzeby i wymagania Zamawiającego, takie jak zgodność z regulacjami, kluczowe punkty monitorowania, typy zagrożeń, na które należy zwracać szczególną uwagę, oraz priorytety w zakresie analizy logów.
- Należy zaplanować odpowiedni sprzęt i zasoby: Ustalić odpowiednią infrastrukturę sprzętową i zasoby, które będą niezbędne do wdrożenia oprogramowania. Uwzględnić wymagania dotyczące serwera, pamięci masowej, sieci i innych zasobów, aby zapewnić wydajność systemu oraz odpowiednią konfigurację i wydajność maszyny wirtualnej.
- Następnie prace wdrożeniowe obejmą przygotowanie środowiska, w ramach których: Należy zainstalować serwer centralny: Zainstalować i skonfigurować serwer centralny, który będzie odpowiedzialny za centralizację logów, ich przetwarzanie oraz zarządzanie oprogramowaniem. Serwer powinien mieć odpowiednią moc obliczeniową oraz wystarczającą przestrzeń dyskową do przechowywania zebranych logów – należy określić wszystkie niezbędne zasoby.
- Należy skonfigurować agentów na urządzeniach końcowych: Na wszystkich serwerach, komputerach oraz innych urządzeniach, które będą generować logi, zainstalować i skonfigurować agentów do zbierania danych. Agenci muszą być dostosowani do specyficznych systemów operacyjnych i urządzeń.
- Należy utworzyć połączenia sieciowe: Upewnić się, że wszyscy agenci są poprawnie połączeni z serwerem centralnym. Połączenia powinny być zabezpieczone, aby zapewnić integralność i poufność przesyłanych danych.
- W następnym kroku prace wdrożeniowe powinny objąć konfigurację zbierania i przetwarzania logów, w ramach których: Należy skonfigurować zbieranie logów z różnych źródeł: Ustawić oprogramowanie tak, aby zbierało logi z serwerów, przełączników, routerów, firewalli oraz innych urządzeń sieciowych. Należy upewnić się, że logi są zbierane w czasie rzeczywistym, a system wspiera różnorodne formaty logów (np. syslog, plain text).

- Należy ustalić reguły filtracji i transformacji logów: Zdefiniować zasady filtracji, które określą, jakie logi mają być przechowywane i analizowane. Oprogramowanie powinno być skonfigurowane do transformacji logów, tak aby dane były normalizowane i wzbogacane o dodatkowe informacje, takie jak metadane czy lokalizacja geograficzna.
- Należy zaimplementować korektę i deduplikację logów: Zaimplementować mechanizmy deduplikacji, które będą eliminować powtarzające się zdarzenia, zapobiegając generowaniu zbędnych alarmów i umożliwiając bardziej efektywną analizę.
- Następnie prace wdrożeniowe skupić się powinny na ustawieniu reguł korelacji i detekcji, w ramach których: Należy skonfigurować reguły korelacji: Ustawić reguły korelacji, które pozwolą na analizę logów pochodzących z różnych źródeł w celu wykrywania bardziej złożonych zagrożeń. Reguły te powinny być dostosowane do specyfiki sieci Urzędu Gminy Lisewo oraz Centru Usług Społecznych w Lisewie.
- Należy zdefiniować sygnatury i anomalie: Zaimplementować reguły wykrywania zagrożeń zarówno na podstawie sygnatur, jak i anomalii. System powinien być w stanie identyfikować znane wzorce zagrożeń oraz odchylenia od normalnego zachowania systemu.
- Należy skonfigurować poziomy krytyczności: Określić poziomy krytyczności dla różnych rodzajów zdarzeń, aby umożliwić priorytetyzację alarmów. Dostosować poziomy krytyczności do wymagań Zamawiającego uwzględniając lokalne regulacje i polityki.
- W ramach wdrożenia wymaganych od Wykonawcy jest implementacja mechanizmów alarmowania, w ramach których: Należy skonfigurować alerty w czasie rzeczywistym: Ustalić mechanizmy generowania alertów w czasie rzeczywistym, które będą informować administratorów o wykrytych zagrożeniach. Alerty powinny być wysyłane za pomocą e-maila.
- Należy ustawić logikę alarmów: Zdefiniować logikę, która będzie decydować, kiedy i w jaki sposób generowane są alarmy. Należy upewnić się, że alarmy są kontekstowe i że system łączy powiązane zdarzenia w celu zredukowania liczby fałszywych pozytywów.
- W celu wdrożenia monitorowania i analizy historycznej: Należy skonfigurować dashboards monitorujące: Utworzyć interaktywne dashboards do monitorowania logów i alarmów w czasie rzeczywistym. Dashboards powinny być dostosowane do potrzeb Zamawiającego umożliwiając łatwe śledzenie kluczowych wskaźników bezpieczeństwa.
- Należy skonfigurować mechanizmy archiwizacji i analizy logów: Skonfigurować mechanizmy archiwizacji logów, które pozwolą na ich długoterminowe przechowywanie i analizę historyczną. Należy zapewnić możliwość przeszukiwania archiwalnych logów w celu prowadzenia audytów i dochodzeń po incydentach.
- Należy zaimplementować generowanie raportów zgodności: Zaimplementować automatyczne generowanie raportów zgodności, które będą odzwierciedlać wymagania regulacyjne, takie jak RODO, i które będą regularnie dostarczane do odpowiednich wydziałów urzędu.
- Dodatkowo należy przygotować oprogramowanie do integracji z innymi systemami poprzez konfigurację integracji z Elastic Stack umożliwiając wizualizację danych logów w Kibana. Dodatkowo, należy zaimplementować API RESTful, które umożliwi integrację oprogramowania z innymi systemami zarządzania incydentami oraz automatyzację procesów związanych z analizą logów.

- W końcowej fazie wdrożenia przed uruchomieniem produkcyjnym oprogramowania należy przeprowadzić testowanie i optymalizację oprogramowania, tj.: Wykonać testy funkcjonalne, aby upewnić się, że wszystkie komponenty modułu działają poprawnie. Testy powinny obejmować zbieranie logów, ich analizę, generowanie alarmów oraz integrację z innymi systemami.
- Przeprowadzić testy obciążeniowe, aby sprawdzić, czy system działa wydajnie nawet przy dużej ilości generowanych logów. Należy upewnić się, że serwer centralny jest w stanie obsłużyć przewidywaną ilość danych.
- Na podstawie wyników testów dokonać niezbędnych optymalizacji, takich jak dostosowanie filtrów, reguł korelacji czy poziomów krytyczności, aby system działał zgodnie z oczekiwaniami Zamawiającego.
- W ramach wdrożenia oprogramowania do agregacji logów należy przeprowadzić szkolenie administratorów odpowiedzialnych za obsługę oprogramowania obejmujące wszystkie aspekty jego konfiguracji, monitorowania i zarządzania incydentami oraz sporządzić szczegółową dokumentację konfiguracji modułu, w tym opis wszystkich zdefiniowanych reguł, schematów połączeń oraz procedur zarządzania systemem.

2) CZĘŚĆ 2 - Dostawa urządzenia sieciowego

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.

Redundancja, monitoring i wykrywanie awarii

- W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastry Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
- Monitoring stanu realizowanych połączeń VPN.
- System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

- System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 16 portami Gigabit Ethernet RJ-45,
 - 1 gniazdem Management RJ-45,
 - 1 gniazdem HA RJ-45,
 - 8 gniazdami SFP 1 Gbps.
 - 4 gniazdami SFP+ 10 Gbps obsadzone wkładkami 10GE SFP+ MM SR kompatybilnymi z urządzeniem – dopuszczalne zamienniki,
- System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
- System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- System jest wyposażony w nadmiarowe zasilanie AC.

Parametry wydajnościowe:

- W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.
- Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.
- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
- Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 256 nie mniej niż 33 Gbps.
- 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 5 Gbps.
- Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

- Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
- Kontrola Aplikacji.
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
- Ochrona przed malware.

- Ochrona przed atakami - Intrusion Prevention System.
- Kontrola stron WWW.
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
- Zarządzanie pasmem (QoS, Traffic shaping).
- 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.
- Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
- Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
- 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

- Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- 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.
- W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
- Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
- Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
- 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

- System 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.
- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec 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:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

- System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- System daje możliwość określania pasma dla poszczególnych aplikacji.

- System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
- System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

- Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
- W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
- System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
- System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
- Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- System 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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.
- System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
- Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
- Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

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

- Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

- Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
- Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
- 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

- Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- 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.
- Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
- Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
- Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
- Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
- Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
- System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

- System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

- Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
 - System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
 - 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.
 - Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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

Logowanie

- 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.
- 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.

- Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
- Możliwość włączenia logowania per reguła w polityce firewall.
- System zapewnia możliwość logowania do serwera SYSLOG.
- Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

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

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 do 30.06.2026.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres do 30.06.2026 r., 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.

4. Wykonawca zobowiązany jest do zaoferowania urządzeń o parametrach nie gorszych niż wymagane w pkt.3.
5. Wykonawca dostarczy przedmiot zamówienia fabrycznie nowy, nieużywany, sprawny technicznie, bez wad fizycznych i prawnych, nigdy wcześniej nie używany. Wszystkie urządzenia stanowiące przedmiot zamówienia powinny być gotowe do pracy, pochodzić z bieżącej produkcji, z legalnego źródła dystrybucji oraz posiadać gwarancję umożliwiającą realizację uprawnień z tytułu gwarancji na terytorium Polski.
6. Dostarczony sprzęt powinien posiadać deklarację zgodności CE zgodnie z obowiązującymi w tym zakresie przepisami.
7. Ilekroć przedmiot zamówienia został opisany za pomocą norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne, pod warunkiem spełnienia przez produkt wymagań określonych we wskazanej normie, ocenie technicznej, specyfikacji technicznej i systemie referencji technicznych, co Wykonawca jest zobowiązany wykazać składając ofertę.
8. Oprogramowanie musi być oryginalne i licencjonowane zgodnie z prawem, nowe i wcześniej nie aktywowane.

9. Podwykonawcy

- 1) Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia. W przypadku powierzenia części zamówienia Podwykonawcom, Wykonawca winien wskazać w ofercie te części zamówienia oraz podać nazwy tych Podwykonawców (o ile są mu znane na danym etapie postępowania).
- 2) Powierzenie wykonania części przedmiotu zamówienia podwykonawcom, nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.

3) Zamawiający nie korzysta z uprawnienia o którym mowa w art.462 ust.5 ustawy PZP, tj. w przypadku powierzenia wykonania części przedmiotu zamówienia podwykonawcom, Zamawiający nie będzie badać, czy nie zachodzą wobec podwykonawcy niebędącego podmiotem udostępniającym zasoby podstawy wykluczenia z niniejszego postępowania.

W związku z powyższym, Zamawiający nie żąda złożenia oświadczenia o braku podstaw wykluczenia i spełnieniu warunków udziału w postępowaniu, lub podmiotowych środków dowodowych dotyczących podwykonawców.

10. Obowiązek podatkowy

Jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, w takim przypadku składając ofertę, informuje Zamawiającego, że wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

CZĘŚĆ IV. TERMIN WYKONANIA ZAMÓWIENIA I WARUNKI PŁATNOŚCI

1. Wykonawca jest zobowiązany wykonać zamówienie w terminie: **max 90 dni od daty zawarcia umowy.**
2. Zapłata wynagrodzenia nastąpi na rachunek zgodnie z postanowieniami Wzoru Umowy, stanowiącego załącznik nr 9 do SWZ.

CZĘŚĆ V. PODSTAWY WYKLUCZENIA

1. Z postępowania o udzielenie zamówienia zgodnie z art.108 ust.1 ustawy wyklucza się Wykonawcę:
 - 1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art.258 Kodeksu karnego,
 - b) handlu ludźmi, o którym mowa w art.189a Kodeksu karnego,
 - c) o którym mowa w art.228–230a, art.250a Kodeksu karnego, w art.46–48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2024 r. poz.1488 z późn. zm.) lub w art.54 ust.1–4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2024 r. poz.930 z późn. zm.),
 - d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
 - e) o charakterze terrorystycznym, o którym mowa w art.115 §20 Kodeksu karnego, lub

mające na celu popełnienie tego przestępstwa,

- f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art.9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2021 r. poz.1745 z późn. zm.),
- g) przeciwko obrotowi gospodarczemu, o których mowa w art.296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art.286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art.270–277d Kodeksu karnego, lub przestępstwo skarbowe,
- h) o którym mowa w art.9 ust.1 i 3 lub art.10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

– lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

- 2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1);
 - 3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - 4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
 - 5) jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
 - 6) jeżeli, w przypadkach, o których mowa w art.85 ust.1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia.
2. Dodatkowo Zamawiający wykluczy Wykonawcę, w stosunku do którego zachodzi którakolwiek z okoliczności, których mowa w art.109 ust.1 pkt.4 ustawy PZP:
- 1) na podstawie art.109 ust.1 pkt.4 ustawy PZP tj.: w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca

wszczęcia tej procedury;

3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art.108 ust.1 pkt.1, 2 i 5 oraz art.109 ust.1 pkt.4 jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:
- 1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne,
 - 2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub Zamawiającym,
 - 3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
 - zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie Wykonawcy,
 - zreorganizował personel,
 - wdrożył system sprawozdawczości i kontroli,
 - utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
 - wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.
 - 4) Zamawiający oceni, czy podjęte przez Wykonawcę czynności, o których mowa w pkt.3 niniejszego rozdziału SWZ, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy.

Jeżeli podjęte przez Wykonawcę czynności, o których mowa w pkt.3 niniejszego rozdziału SWZ, nie są wystarczające do wykazania jego rzetelności, Zamawiający wyklucza Wykonawcę na podstawie art.111 ustawy PZP.

4. W zakresie podstaw wykluczenia zastosowanie znajdują również odpowiednie zapisy art.110 oraz art.111 ustawy.
5. Ponadto z postępowania wyklucza się Wykonawcę 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. z 2025 r. poz.514). Wykonawca dołączy do oferty Oświadczenie zgodne ze wzorem stanowiącym załącznik nr 5 SWZ.
6. Wykluczenie, o którym mowa w ust.5, następuje na okres trwania okoliczności określonych w ust.5.
7. W przypadku wykonawcy wykluczonego na podstawie ust.5, zamawiający odrzuca ofertę takiego wykonawcy na podstawie art.7 ust.3 ustawy o szczególnych rozwiązaniach.

CZĘŚĆ VI. INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu dotyczące:

- 1) zdolności do występowania w obrocie gospodarczym:

Zamawiający nie stawia warunku w ww. zakresie.

- 2) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:

Zamawiający nie stawia warunku w ww. zakresie.

- 3) sytuacji ekonomicznej lub finansowej:

Zamawiający nie stawia warunku w ww. zakresie.

- 4) zdolności technicznej lub zawodowej:

Wykonawca spełni warunek dotyczący zdolności technicznej lub zawodowej, jeżeli:

- w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie należycie wykonał lub należycie wykonuje co najmniej:
- dla części 1: 2 dostawy serwerów i macierzy o wartości nie mniejszej niż **100 000,00 zł brutto każda;**
- dla części 2: 2 dostawy urządzeń sieciowych o wartości nie mniejszej niż **15 000,00 zł brutto każda;**

2. Oceniając zdolność techniczną lub zawodową, 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.
3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia warunki, o których mowa w ust.1 niniejszej części SWZ zostaną spełnione wyłącznie jeżeli w odniesieniu do zdolności technicznej, o której mowa w ust.1 pkt.4 niniejszej części SWZ jeden z wykonawców spełni warunek samodzielnie lub Wykonawcy spełnią warunek łącznie.
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 lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
5. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów (**załącznik nr 8 do SWZ**).
6. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust.5, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
 - 1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;

- 2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
7. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w art.112 ust. 2 pkt 4 ustawy, oraz, jeżeli to dotyczy, kryteriów selekcji, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
8. Podmiot, który zobowiązał się do udostępnienia zasobów, odpowiada solidarnie z Wykonawcą, który polega na jego sytuacji finansowej lub ekonomicznej, za szkodę poniesioną przez Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów podmiot ten nie ponosi winy.
9. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
10. Wykonawca nie może, po upływie terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania wniosków o dopuszczenie do udziału w postępowaniu albo ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
11. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust.5 składa się w formie zgodnej z postanowieniami rozporządzeń, o których mowa w części VII ust. 15 SWZ.
12. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty Oświadczenie, z którego wynikać będzie, które roboty wykonają poszczególni wykonawcy.
Oświadczenie należy złożyć zgodnie ze wzorem stanowiącym załącznik nr 4 do SWZ.
13. W przypadku, gdy Wykonawcy wspólnie ubiegają się o udzielenie zamówienia, to Wykonawcy ci ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego oraz ponoszą solidarną odpowiedzialność za wykonanie umowy.
14. **Art.118 ust.1 ustawy nie przewiduje polegania na zdolnościach podmiotów udostępniających zasoby w celu potwierdzenia spełniania warunków udziału w postępowaniu dot. posiadania uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej.**

CZĘŚĆ VII. PODMIOTOWE ŚRODKI DOWODOWE ORAZ PRZEDMIOTOWE ŚRODKI DOWODOWE

1. Do oferty każdy Wykonawca musi dołączyć aktualne na dzień składania ofert oświadczenie o niepodleganiu wykluczeniu z postępowania w zakresie wskazanym przez Zamawiającego – wzór stanowi załącznik nr 2 do SWZ oraz oświadczenie o spełnianiu warunków udziału w postępowaniu – wzór stanowi załącznik nr 3 do SWZ, w zakresie wskazanym przez

zamawiającego.

2. Oświadczenia, o których mowa powyżej w ust.1 stanowią dowód potwierdzający brak podstaw do wykluczenia oraz spełnianie warunków udziału w postępowaniu na dzień składania ofert, tymczasowo zastępujący wymagane przez zamawiającego podmiotowe środki dowodowe (o ile są one wymagane przez Zamawiającego).
3. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenia, o których mowa w ust.1, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
4. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniami, o których mowa w ust. 1, także oświadczenia podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby.
5. Zamawiający wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, aktualnych na dzień złożenia podmiotowych środków dowodowych:

1) w zakresie potwierdzenia braku podstaw wykluczenia z postępowania:

- a) odpisu lub informacji 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;
- b) **oświadczenia Wykonawcy**, w zakresie **art.108 ust.1 pkt.5** ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2024 r. poz.1616), z innym Wykonawcą, który złożył odrębną ofertę, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej, zgodnie ze wzorem stanowiącym Załącznik nr 6 do SWZ.
- c) oświadczenia złożonego 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. z 2025 r. poz.514) zgodnie ze wzorem stanowiącym załącznik nr 5 SWZ.

2) w zakresie spełnienia warunków udziału w postępowaniu:

- a) Wykaz dostaw wykonanych a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane należycie (**załącznik nr 7 SWZ**), oraz załączeniem dowodów określających 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, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy.

6. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument poza granicami Rzeczypospolitej Polskiej, zamiast:
 - 1) odpisu albo informacji z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w ust.5 pkt.1 – składa się dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
 - a) nie otwarto 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. Dokumenty powinny być wystawione nie wcześniej niż 3 miesiące przed ich złożeniem.
7. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w ust.5 lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art.108 ust.1, 2, 4 ustawy, 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 lub miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego i gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy lub miejsce zamieszkania osoby, której dokument miał dotyczyć. Terminy określone w ust.5 stosuje się.
8. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli 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 ustawy, dane umożliwiające dostęp do tych środków.
9. Jeżeli Wykonawca nie złożył oświadczeń, o których mowa ust.1 niniejszej części, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wezwie Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że:
 - 1) oferta Wykonawcy podlega odrzuceniu bez względu na jego złożenie, uzupełnienie lub poprawienie lub
 - 2) zachodzą przesłanki unieważnienia postępowania.

10. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści oświadczenia, o którym mowa w ust.1, lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu.
11. Wraz z ofertą Wykonawca musi złożyć następujące przedmiotowe środki dowodowe:
 - 1) Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych.
12. Jeżeli Wykonawca nie złożył przedmiotowych środków dowodowych, o których mowa powyżej lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
13. Postanowienia, o którym mowa w ust. 12 nie stosuje się, jeżeli oferta Wykonawcy podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.
14. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowych.
15. W zakresie nie uregulowanym niniejszą SWZ, zastosowanie mają przepisy:
 - 1) 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 (Dz. U. z 2020 r., poz. 2415);
 - 2) 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 (Dz. U. z 2020 r., poz. 2452).

CZĘŚĆ VIII. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się za pomocą poczty elektronicznej e-mail: ab@powiat-sepolno.pl (nie dotyczy składania ofert o dopuszczenie do udziału w postępowaniu) oraz przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem <https://ezamowienia.gov.pl> (złożenie oferty następuje wyłączenie przy użyciu Platformy e-Zamówienia).
2. Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:
 - 1) W sprawach merytorycznych: **Wojciech Bilski**
 - 2) W sprawach formalnych: **Tomasz Bondarczyk**Adres poczty elektronicznej e-mail: ab@powiat-sepolno.pl
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. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w rozporządzeniu 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 w konkursie (Dz. U. z 2020 r. poz.2452) zwanym dalej „*rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych*”.
6. Dokumenty elektroniczne, o których mowa w §2 ust.1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, a wymagane zapisami SWZ, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) zwanym dalej „*rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności*”, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki.
7. Informacje, oświadczenia lub dokumenty, inne niż wymienione w §2 ust.1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, przekazywane w postępowaniu sporządza się w postaci elektronicznej:
 - 1) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (i przekazuje się jako załącznik), lub
 - 2) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści „Formularza do komunikacji”).
8. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów 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 zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”.
9. Komunikacja w postępowaniu, z wyłączeniem składania ofert/wniosków o dopuszczenie do udziału w postępowaniu, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze” („Formularze do komunikacji”). Za pośrednictwem „Formularzy do komunikacji” odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik”). Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na adres email: ab@powiat-sepolno.pl
10. W przypadku załączników, które są zgodnie z ustawą lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone,

zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem zewnętrznym lub wewnętrznym. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się do przesyłanej wiadomości uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).

11. Możliwość korzystania w postępowaniu z „Formularzy do komunikacji” w pełnym zakresie wymaga posiadania konta „Wykonawcy” na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z „Formularzy do komunikacji” służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e-Zamówienia.
12. Wszystkie wysłane i odebrane w postępowaniu przez wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja”.
13. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
14. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
15. 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”.
16. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
17. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert albo ofert podlegających negocjacjom, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania odpowiednio ofert albo ofert podlegających negocjacjom.
18. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 17, przedłuża termin składania odpowiednio ofert albo ofert podlegających negocjacjom o czas niezbędny do zapoznania się wszystkich zainteresowanych Wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia odpowiednio ofert albo ofert podlegających negocjacjom.
19. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust.17, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania odpowiednio ofert albo ofert podlegających negocjacjom.
20. Przedłużenie terminu składania ofert, o których mowa w ust.18, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
21. Treść pytań wraz z wyjaśnieniami Zamawiający udostępnia, bez ujawniania źródła zapytania, na stronie internetowej prowadzonego postępowania.

CZĘŚĆ IX. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie żąda wniesienia wadium.

CZĘŚĆ X. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca będzie związany ofertą do dnia **20 stycznia 2026 r.** 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 określonego w SWZ, 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, o którym mowa w ust.2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. W przypadku gdy Zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, o którym mowa w ust. 2, następuje wraz z przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

CZĘŚĆ XI. OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Wykonawca może złożyć tylko jedną ofertę.
2. Ofertę należy sporządzić w języku polskim.
Wykonawca przygotowuje ofertę przy pomocy *Formularza oferty* stanowiącego załącznik nr 1 do SWZ uzupełniając go o dane wymagane przez Zamawiającego.
Uwaga! Zamawiający nie udostępnia interaktywnego formularza ofertowego na Platformie e-Zamówienia i w związku z tym należy zignorować komunikat pojawiający się przy składaniu oferty w tym zakresie.
3. Wykonawca składa ofertę za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto Wykonawcy na Platformie e-Zamówienia. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola drag&drop („przeciągnij” i „upuść”) służące do dodawania plików.
4. Wykonawca dodaje wybrany z dysku i uprzednio podpisany „Formularz oferty” w pierwszym polu („Wypełniony formularz oferty”). W kolejnym polu („Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”) wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
5. Jeżeli wraz z ofertą składane są dokumenty zawierające tajemnicę przedsiębiorstwa wykonawcy, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”. Zarówno załącznik stanowiący tajemnicę przedsiębiorstwa jak i uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa należy dodać w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.
6. Zamawiający informuje, że nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz.1233), jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o

których mowa w art. 222 ust. 5 ustawy.

7. *Formularz oferty* podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Rekomendowanym wariantem podpisu jest typ wewnętrzny. Podpis formularza ofertowego wariantem podpisu w typie zewnętrznym również jest możliwy, tylko w tym przypadku, powstały oddzielny plik podpisu dla tego formularza należy załączyć w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.
8. Pozostałe dokumenty wchodzące w skład oferty lub składane wraz z ofertą, które są zgodne z ustawą Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby opatrzone podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę” dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
9. W przypadku przekazywania dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
10. System sprawdza, czy złożone pliki są podpisane i automatycznie je szyfruje, jednocześnie informując o tym wykonawcę. Potwierdzenie czasu przekazania i odbioru oferty znajduje się w Elektronicznym Potwierdzeniu Przesłania (EPP) i Elektronicznym Potwierdzeniu Odebrania (EPO). EPP i EPO dostępne są dla zalogowanego Wykonawcy w zakładce „Oferty/Wnioski”.
11. Oferta może być złożona tylko do upływu terminu składania ofert.
12. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „Oferty/wnioski” używając przycisku „Wycofaj ofertę”.
13. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.
14. Zamawiający żąda wskazania przez wykonawcę, w *Formularzu oferty* (w miejscu do tego przeznaczonym), części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, oraz podania nazw ewentualnych podwykonawców, jeżeli są już znani. Brak wskazania części zamówienia, o którym mowa w zdaniu poprzednim zostanie uznany za stwierdzenie samodzielnego wykonania zamówienia przez Wykonawcę.
15. Wraz z ofertą należy złożyć dokumenty i oświadczenia, o których mowa w części VII ust.1 SWZ oraz zobowiązanie i oświadczenie, o których mowa w części VI ust.5 i 12 SWZ, a także pełnomocnictwa lub inne dokumenty potwierdzające umocowanie do reprezentacji zgodnie z postanowieniami części XI SWZ.
16. 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. W przypadku, gdy dokumenty potwierdzające umocowanie do

reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art.118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „upoważnionymi podmiotami”, jako dokument elektroniczny, przekazuje się ten dokument. W przypadku gdy dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w zdaniu poprzednim, dokonuje odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej może dokonać również notariusz. Przez cyfrowe odwzorowanie należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.

17. Wykonawca nie jest zobowiązany do złożenia dokumentów, o których mowa w ust.16, jeżeli zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile wykonawca wskazał dane umożliwiające dostęp do tych dokumentów. Zamawiający będzie żądać od wykonawcy przedstawienia tłumaczenia na język polski pobranych samodzielnie przez zamawiającego dokumentów.
18. Jeżeli w imieniu wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów, o których mowa w ust.16, zamawiający żąda od wykonawcy pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania wykonawcy.
19. Przepis ust.16 stosuje się odpowiednio do osoby działającej w imieniu wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego.
20. Przepisy ust.16–18 stosuje się odpowiednio do osoby działającej w imieniu podmiotu udostępniającego zasoby na zasadach określonych w art.118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach.
21. Pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. W przypadku gdy pełnomocnictwo zostało 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. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w zdaniu poprzednim, dokonuje mocodawca lub notariusz.
22. W przypadku załączenia do oferty dokumentów i oświadczeń sporządzonych w języku obcym

przekazuje się wraz z tłumaczeniem na język polski.

CZEŚĆ XII. SPOSÓB ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. **Termin składania ofert upływa dnia 22 grudnia 2025 r. o godz. 8:30**
2. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
3. **Otwarcie ofert nastąpi dnia 22 grudnia 2025 r. o godz. 9:00.**
4. Otwarcie ofert następuje za pomocą Platformy e-Zamówienia.
5. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
6. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informację 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.
7. W przypadku wystąpienia awarii systemu teleinformatycznego, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
8. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania lub w przypadku awarii strony prowadzonego postępowania na stronie Zamawiającego: <https://www.bip.powiat-sepolno.pl>
9. Zamawiający nie przewiduje przeprowadzenia jawnej sesji otwarcia ofert.

CZEŚĆ XIII. SPOSÓB OBLICZENIA CENY

1. Zamawiający ustala, że obowiązującym rodzajem wynagrodzenia w przedmiotowym zamówieniu jest wynagrodzenie ryczałtowe w rozumieniu art.632 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. 2024 poz. 1061 ze zm.).
2. Cena ofertowa powinna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia uwzględniające cały zakres przedmiotu zamówienia oraz ewentualne ryzyko wynikające z okoliczności, które można było przewidzieć w terminie opracowywania oferty do czasu jej złożenia oraz wszystkie inne koszty towarzyszące m. in. koszty dostawy, ubezpieczenie transportu oraz wszystkie inne koszty, które będą musiały być poniesione przy wykonaniu zamówienia w tym podatków i opłat.
3. Wykonawca musi zaoferować cenę jednoznaczną i ostateczną, która nie będzie podlegała negocjacjom przy podpisaniu Umowy.
4. Cena ofertowa brutto = cena netto + podatek VAT
6. Cena ofertowa musi być podana w zł (PLN) cyfrowo z wyodrębnieniem należnego podatku VAT.
7. Cena ofertowa powinna być aktualna na dzień składania ofert.
8. Wszystkie rozliczenia pomiędzy Zamawiającym, a Wykonawcą dokonywane będą w złotych polskich. W złożonej ofercie Wykonawca zobowiązany jest podać właściwą stawkę podatku od towarów i usług VAT, zgodną z obowiązującymi Wykonawcę przepisami.
9. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

10. Zaoferowana cena nie podlega zmianom przez okres obowiązywania umowy z wyjątkiem ustawowej zmiany stawki podatku VAT.

11. Cenę oferty oraz pozostałe wartości należy przedstawić z dokładnością do dwóch miejsc po przecinku przy zachowaniu matematycznej zasady zaokrąglania liczb. Kwoty zaokrągla się do pełnych groszy, przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki od 0,5 grosza zaokrągla się do 1 grosza.

12. 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 2025 r. poz. 775), dla celów zastosowania kryterium ceny lub kosztu Zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałyby obowiązek rozliczyć.

13. W ofercie, o której mowa w ust. 12, Wykonawca ma obowiązek:

- a) poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
- b) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
- c) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;
- d) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

CZĘŚĆ XIV. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Przy ocenie złożonych ofert Zamawiający kierować się będzie następującymi kryteriami:

RODZAJ KRYTERIUM

WAGA KRYTERIUM

1. Cena

60%

2. Termin realizacji

40%

2. Kryterium „cena” rozpatrywane będzie na podstawie ceny podanej przez Wykonawcę w formularzu ofertowym – załącznik nr 1 SIWZ. Zamawiający stosuje zaokrąglenie każdego wyniku do dwóch miejsc po przecinku.

3. Kryterium „Termin realizacji” będzie rozpatrywane na podstawie określonego terminu dostawy przez Wykonawcę w formularzu ofertowym – załącznik nr 1 SWZ.

4. Ocena punktowa będzie dotyczyć wyłącznie ofert uznanych za ważne i niepodlegające odrzuceniu.

5. Sposób oceniania ofert:

- a) kryterium cena rozpatrywane będzie na podstawie ceny ryczałtowej podanej przez Wykonawcę w formularzu ofertowym wg następującego wzór (C):

$$C = \frac{\text{cena oferty najkorzystniejszej}}{\text{cena oferty badanej}} \times 60$$

Wykonawca w kryterium cena otrzyma max. 60 pkt.

b) kryterium „termin realizacji” rozpatrywane będzie na podstawie określonego terminu dostawy w formularzu cenowym (T):

Zamawiający przyzna **40 pkt** – za termin realizacji do 60 dni od daty zawarcia umowy

Zamawiający przyzna **30 pkt** – za termin realizacji do 70 dni od daty zawarcia umowy

Zamawiający przyzna **20 pkt** – za termin realizacji do 80 dni od daty zawarcia umowy

Zamawiający przyzna **10 pkt** – za termin realizacji do 90 dni od daty zawarcia umowy

Maksymalny termin realizacji zamówienia wynosi 90 miesięcy od daty zawarcia umowy.

W przypadku zaoferowania terminu realizacji innego, niż podany wyżej, w celu ustalenia punktacji w tym kryterium, termin realizacji zostanie zaokrąglony do najbliższego terminu podanego wyżej w dół (np. przy wskazaniu terminu realizacji 62 dni Wykonawca otrzyma 30 pkt.).

Jeśli Wykonawca nie wskaże w ofercie terminu realizacji Zamawiający przyjmie, że zaoferowano termin wynoszący 90 dni.

Wykonawca w kryterium „termin realizacji” otrzyma max. 40 pkt.

c) Łączny bilans punktowy uzyskany w kryteriach:

$$C + T = \text{ilość otrzymanych punktów}$$

6. Zamawiający przyzna zamówienie Wykonawcy, którego oferta odpowiada zasadom określonym w Ustawie i spełnia wymagania określone w SWZ oraz została uznana za najkorzystniejszą.
7. Zamawiający informuje niezwłocznie wszystkich Wykonawców o:
 - 1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo adres zamieszkania, jeżeli jest miejscem wykonywania działalności Wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację;
 - 2) wykonawcach, których oferty zostały odrzucone,
 - 3) unieważnieniu postępowania podając uzasadnienie faktyczne i prawne.
8. Zamawiający udostępni informacje, o których mowa w pkt.7 na stronie internetowej prowadzonego postępowania.
9. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert, Zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze.
10. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, Zamawiający wybiera

ofertę z najniższą ceną lub najniższym kosztem.

11. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa w ust.10, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę lub koszt.
12. Wykonawcy, składając oferty dodatkowe, nie mogą oferować cen lub kosztów wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.
13. Zamawiający uzna za ofertę najkorzystniejszą, ofertę, która uzyska najwyższą ostateczną wartość punktową z zastrzeżeniem treści ust. 9-12 powyżej.

CZĘŚĆ XV. INFORMACJA O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art.577, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli złożono tylko jedną ofertę.
3. Podpisanie Umowy nastąpi w miejscu i czasie wskazanym przez Zamawiającego.
4. W przypadku, gdy z dokumentów załączonych do oferty nie wynika uprawnienie do zawarcia umowy, Wykonawca zobowiązany będzie do przedstawienia takiego dokumentu przez zawarciem umowy.
5. Jeżeli została wybrana oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie (art.263 ustawy Pzp).

CZĘŚĆ XVI. INFORMACJE DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

CZĘŚĆ XVII. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI UMOWY

Zamawiający zawrze umowę zgodnie ze wzorem Umowy stanowiącej załącznik nr 9 do SWZ.

CZĘŚĆ XVIII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej określone w dziale IX ustawy 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.
2. 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, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:
 - 1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania Wykonawców lub konkursie, w tym na projektowane postanowienie umowy;
 - 2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania Wykonawców lub konkursie, do której Zamawiający był obowiązany na podstawie ustawy;
 - 3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że Zamawiający był do tego obowiązany.
4. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „*Środki ochrony prawnej*” ustawy.

CZĘŚĆ XIX. OFERTY WARIANTOWE I CZĘŚCIOWE ORAZ INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT 8 USTAWY

1. Zamawiający nie dopuszcza możliwości składania oferty wariantowej.
2. Zamawiający dopuszcza możliwości składania ofert częściowych.
3. Zamawiający nie przewiduje możliwości udzielenia zamówienia dotychczasowemu Wykonawcy robót, o których mowa w art.214 ust.1 pkt.8 ustawy PZP.
4. Zamawiający nie przewiduje ustanowienia dynamicznego systemu zakupów.
5. Przedmiotem niniejszego postępowania nie jest zawarcie umowy ramowej.
6. Zamawiający nie przewiduje zastosowania aukcji elektronicznej.
7. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
8. Zamawiający nie określił w opisie przedmiotu zamówienia wymagań w zakresie zatrudnienia osób, o których mowa w art.96 ust.2 pkt.2 ustawy.
9. Zamawiający nie przewiduje zastrzeżenia możliwości ubiegania się o udzielenie zamówienia wyłączenie przez Wykonawców, o których mowa w art.94 ustawy Pzp.
10. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia. W przypadku powierzenia części zamówienia Podwykonawcom, Wykonawca winien wskazać w ofercie te części zamówienia oraz podać nazwy tych Podwykonawców (o ile są mu znane na danym etapie postępowania).
11. Zamawiający nie przewiduje złożenia oferty w postaci katalogów elektronicznych.
12. Zamawiający nie przewiduje zastosowania opcji zgodnie z art.441 ust.1 ustawy Pzp.

CZĘŚĆ XX. POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w niniejszej SWZ zastosowanie mają przepisy ustawy Prawo zamówień publicznych, Kodeksu cywilnego oraz obowiązujące przepisy wykonawcze.

CZĘŚĆ XXI. INFORMACJA O OCHRONIE DANYCH (RODO)

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 ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- 1) administratorem Pani/Pana danych osobowych jest *Starosta Sępoleński – ul. Kościuszki 11, 89-400 Sępólno Kraj. tel. 52 388 13 00*;
- 2) inspektorem ochrony danych osobowych w Starostwie Powiatowym jest Pani Anna Kuchna, *iod@powiat-sepolno.pl, tel. 52 388 13 68* ;
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art.6 ust.1 lit.c i e RODO w celu postępowaniem **znak: AB.272.15.2025**, na **„Dostawę urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat”** ” prowadzonym na podstawie art.275 pkt.1 ustawy Pzp;
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art.18 oraz art.74 ust.1 i 2 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz.1320 ze zm.), dalej „ustawa Pzp”;
- 5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art.78 ust.1 ustawy Pzp, 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;
- 6) obowiązek podania przez Panią/Pana danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- 8) posiada Pani/Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
 - c) 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;
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- 9) nie przysługuje Pani/Panu:
 - a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

c) 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 i e RODO.

CZEŚĆ XXII. ZAŁĄCZNIKI

1. Formularz oferty – załącznik nr 1 do SWZ;
2. Oświadczenie o niepodleganiu wykluczeniu z postępowania - załącznik nr 2 do SWZ;
3. Oświadczenie o spełnianiu warunków udziału w postępowaniu - załącznik nr 3 do SWZ;
4. Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia - załącznik nr 4 do SWZ;
5. Oświadczenie Wykonawcy - załącznik nr 5 do SWZ;
6. Oświadczenie o przynależności do grupy kapitałowej – załącznik nr 6 do SWZ;
7. Wykaz dostaw – załącznik nr 7 do SWZ
8. Zobowiązanie podmiotu udostępniającego zasoby – załącznik nr 8 do SWZ
9. Wzór Umowy - załączniki nr 9 do SWZ.

Pełna Nazwa Wykonawcy/ Wykonawców	
Adres, siedziba	
Adres do korespondencji	
REGON	
NIP	
KRS/CEIDG	
Nr telefonu	
e-mail	
Imię Nazwisko i Nr telefonu osoby upoważnionej do kontaktów	

FORMULARZ OFERTY

Dotyczy postępowania o udzielenie zamówienia pn.

Nazwa postępowania	Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat
Znak sprawy	AB.272.15.2025

1. Oferujemy wykonanie przedmiotu zamówienia zgodnie z opisem i warunkami określonymi w specyfikacji warunków zamówienia:

1)	Część I Cena netto:zł VAT (23%)zł Cena brutto:zł Serwer 1 + oprogramowanie (<i>producent</i>) (<i>model</i>), cena jednostkowa brutto: Macierz dyskowa (<i>producent</i>) (<i>model</i>), cena jednostkowa brutto:
-----------	---

	<p>Serwer 2 + oprogramowanie (<i>producent</i>) (<i>model</i>), cena jednostkowa brutto:</p> <p>Część II</p> <p>Cena netto:zł</p> <p>VAT (23%)zł</p> <p>Cena brutto:zł</p> <p>Urządzenie UTM (<i>producent</i>) (<i>model</i>)</p>
2)	<p>Część I</p> <p>Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera (<i>proszę wskazać link do strony producenta</i>)</p> <p>Adres internetowy strony producenta macierzy (<i>proszę wskazać link do strony producenta</i>)</p>
3)	<p><i>Wybór mojej oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2024 r. poz.361).¹</i></p> <ul style="list-style-type: none"> – nazwa (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego..... – wartość towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku..... - stawka podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.....
4)	<p>Część I</p> <p>Termin realizacji zamówienia: dni od daty zawarcia umowy</p> <p>Część II</p> <p>Termin realizacji zamówienia: dni od daty zawarcia umowy</p> <p><i>(Zamawiający informuje, że termin realizacji nie może być dłuższy niż 90 dni od daty zawarcia umowy)</i></p>

¹ Wykonawca wypełnia jeżeli zastosowanie ma art. 225 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz.1320 z późn. zm.).

2. Jednocześnie oświadczamy, że:

- 1) Zapoznaliśmy się z treścią SWZ oraz wyjaśnieniami i/lub modyfikacjami SWZ i uznajemy się za związanych określonymi w nich postanowieniami i zasadami postępowania.
- 2) Oferowany sprzęt jest zgodny z opisem SWZ.
- 3) Nie wnosimy żadnych zastrzeżeń do treści SWZ.
- 4) Cena oferty zawiera wszystkie koszty niezbędne do wykonania zamówienia określone zapisami SWZ.
- 5) Uważamy się za związanych niniejszą ofertą przez czas wskazany w SWZ.
- 6) Akceptujemy wzór Umowy bez zastrzeżeń i w razie wybrania naszej oferty zobowiązujemy się do zawarcia Umowy na warunkach zawartych w SWZ, w miejscu i terminie wskazanym przez Zamawiającego.
- 7) Wykonanie następujących części zamówienia zamierzamy powierzyć podwykonawcom²:

Lp.	Część zamówienia, którą Wykonawca zamierza powierzyć do realizacji przez podwykonawcę	Firma (nazwa) podwykonawcy

- 8) Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO³ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.⁴
- 9) Jesteśmy mikroprzedsiębiorstwem lub małym przedsiębiorstwem lub średnim przedsiębiorstwem

<input type="checkbox"/> NIE	
<input type="checkbox"/> TAK	(W przypadku zaznaczenia odpowiedzi „tak” należy również wypełnić poniższe dane):
	<input type="checkbox"/> Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.
	<input type="checkbox"/> Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.
	<input type="checkbox"/> Średnie przedsiębiorstwo: przedsiębiorstwo, które nie jest mikroprzedsiębiorstwem ani małym przedsiębiorstwem i które zatrudnia mniej niż 250 osób i którego roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR.

² należy wypełnić jeżeli dotyczy

³ 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).

⁴ 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).

3. Wraz z ofertą składamy następujące oświadczenia i dokumenty:

- 1)
- 2)
- 3)

Nazwa Wykonawcy / Wykonawców

.....

Adres

REGON

NIP

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

Dotyczy postępowania pn:

Nazwa postępowania	Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat
Znak sprawy	AB.272.15.2025

Na potrzeby przedmiotowego postępowania o udzielenie zamówienia publicznego oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania na podstawie art.108 ust.1 pkt.1-6 ustawy oraz art.109 ust.1 pkt.4.

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ustawy (*podać mającą zastosowanie podstawę wykluczenia spośród wymienionych powyżej*). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy podjąłem 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.

Nazwa Wykonawcy / Wykonawców

.....

.....

Adres

REGON

NIP

OŚWIADCZENIE O SPEŁNIANIU WARUNKÓW W POSTĘPOWANIU

(składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako: ustawa)

Dotyczy postępowania pn:

Nazwa postępowania	Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat
Znak sprawy	AB.272.15.2025

Na potrzeby przedmiotowego postępowania o udzielenie zamówienia publicznego oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

Oświadczam, że na dzień składania ofert spełniam warunki udziału w postępowaniu określone przez zamawiającego w części VI SWZ.

INFORMACJA W ZWIAZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w części VI SWZ polegam na zasobach następującego/ych podmiotu/ów:.....

.....
w następującym zakresie:.....

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

Oświadczam, że następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.:

.....

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

nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

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

Oświadczam, że następujący/e podmiot/y, będący/e podwykonawcą/ami:

.....

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

nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia.

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.

**Wykonawcy wspólnie ubiegający
się o udzielenie zamówienia:**

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu:

NIP/PESEL, KRS/CEiDG)

Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia**składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r.****Prawo zamówień publicznych (dalej jako: pzp)**

Dotyczy postępowania pn:

Nazwa postępowania	Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat
Znak sprawy	AB.272.15.2025

Na potrzeby przedmiotowego postępowania o udzielenie zamówienia publicznego oświadczam, co następuje:

- Wykonawca
(nazwa i adres Wykonawcy) zrealizuje następujące dostawy:
.....
- Wykonawca
(nazwa i adres Wykonawcy) zrealizuje następujące dostawy:
.....

Nazwa Wykonawcy / Wykonawców

.....
.....

Adres

REGON

NIP

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

Oświadczenie wykonawcy

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat”** prowadzonego przez Powiat Sępoleński oświadczam, co następuje:

Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia 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. z 2025 r. poz.514)⁵.

⁵ Zgodnie z treścią 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, zwanej dalej „ustawą”, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

- 1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
- 2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz.644) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
- 3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 z późn. zm.), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

Nazwa Wykonawcy / Wykonawców

.....
.....

Adres

REGON

NIP

OŚWIADCZENIE WYKONAWCY

składane na podstawie art.273 ust.1 i ust.2 w zw. z art.108 ust.1 pkt.5 ustawy z dnia
11 września 2019 r. ustawy Prawo zamówień publicznych (dalej ustawa PZP)
o braku przynależności lub przynależności do grupy kapitałowej

Przystępując do udziału w postępowaniu o zamówienie publiczne na:

**„Dostawę urządzeń do backupu, analizy logów oraz urządzenia sieciowego
w ramach projektu Cyberbezpieczny Powiat”**

oświadczam, że podmiot, który reprezentuję:

┌ nie należy do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o
ochronie konkurencji i konsumentów (Dz.U. z 2024 r. poz.1616 z późn. zm.) w stosunku do
Wykonawców, którzy złożyli odrębne oferty w niniejszym postępowaniu o udzielenie
zamówienia publicznego;

┌ należy do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie
konkurencji i konsumentów (Dz.U. z 2024 r. poz.1616 z późn. zm.) z innym Wykonawcą, który
złożył odrębną ofertę w niniejszym postępowaniu o udzielenie zamówienia publicznego.

Nazwa i adres Wykonawcy:

**W przypadku przynależności do tej samej grupy kapitałowej wykonawca może złożyć wraz
z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym
wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu (dotyczy
Wykonawców należących do tej samej grupy kapitałowej, którzy złożyli odrębne oferty w
przedmiotowym postępowaniu o udzielenie zamówienia).**

Nazwa Wykonawcy / Wykonawców

.....

.....

Adres

REGON

NIP

WYKAZ DOSTAW

W związku z postępowaniem na „Dostawę urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat” przedstawiamy wykaz zrealizowanych dostaw:

Lp.	Nazwa i/lub przedmiot zamówienia/dostawa	Zakres zamówienia/dostawy (co najmniej zakres wymagany w warunkach udziału w postępowaniu)	Podmiot na rzecz, którego wykonano zamówienie/dostawę (nazwa i adres)	Wartość brutto dostawy	Daty realizacji (od dd.mm.rrrr do dd.mm.rrrr)
1	2	3	4	5	6
1					
2					

Do niniejszego wykazu należy dołączyć dowody dotyczące wykonanych dostaw, określające, czy dostawy te zostały wykonane w sposób należyty.

Nazwa Wykonawcy / Wykonawców

.....
.....

Adres

REGON

NIP

OŚWIADCZENIE DOTYCZĄCE UDOSTĘPNIENIA ZASOBÓW

Ja niżej podpisany

(imię i nazwisko osoby upoważnionej do reprezentowania podmiotu)

działając w imieniu i na rzecz

(nazwa/firma dokładny adres)

Zobowiązuję się do oddania wymienionych poniżej zasobów na potrzeby wykonania zamówienia:

.....
.....

(określenie zasobu: wiedza i doświadczenie, potencjał techniczny, potencjał kadrowy, potencjał ekonomiczny lub finansowy)

do dyspozycji Wykonawcy

(nazwa Wykonawcy)

przy wykonywaniu niżej wymienionego zamówienia pn: „Dostawa urządzeń do backupu, analizy logów oraz urządzenia sieciowego w ramach projektu Cyberbezpieczny Powiat”

oświadczam, co następuje:

1. Oświadczam, że udostępniam Wykonawcy wyżej wymienione zasoby, w następującym zakresie:

.....

(określenie zasobu: sytuacja finansowa lub ekonomiczna/zdolność techniczna i zawodowa (wiedza i doświadczenie)/osoby (potencjał kadrowy))

2. Oświadczam, że sposób wykorzystania udostępnionych przeze mnie zasobów będzie następujący:

.....

3. Oświadczam, że zakres i okres mojego udziału przy wykonywaniu zamówienia będzie następujący:

.....

4. Oświadczam, że w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuję dostawy, których wskazane zdolności dotyczą.

Projekt umowy

Zawiera się umowę pomiędzy:

Powiatem Sępoleńskim – ul. Kościuszki 11, 89-400 Sępólno Kraj.

REGON, NIP

reprezentowanym przez:

1.

2.

przy kontrasygnacie – Skarbnika Powiatu Sępoleńskiego

zwanym w dalszej części Umowy „**Zamawiającym**”,

a

.....

NIP....., REGON

reprezentowanym przez:

1.

zwanym w dalszej części niniejszej umowy Wykonawcą,

zwanymi dalej łącznie „**Stronami**”, o następującej treści:

§ 1

1. Wykonawca, wyłoniony w postępowaniu o udzielenie zamówienia publicznego, zgodnie ze złożoną ofertą, zobowiązuje się dostarczyć:

Część I:

- **Serwer 1 wraz z oprogramowaniem** (*producent*) (*model*),
- **Macierz dyskową** (*producent*) (*model*),
- **Serwer 2 wraz z oprogramowaniem** (*producent*) (*model*),

Część II

- **Urządzenie UTM** (*producent*) (*model*),

zwanymi dalej „urządzeniami serwerowymi”, których szczegółowy opis zawarto w SWZ.

2. Wykonawca zobowiązuje się dostarczyć do Starostwa Powiatowego w Sępólnie Krajeńskim przedmiot zamówienia, co potwierdzone zostanie protokołem zdawczo-odbiorczym. Wykonawca zobowiązany jest do wcześniejszego ustalenia terminu dostawy, minimum z trzydniowym wyprzedzeniem.
3. Wykonawca zobowiązuje się do realizacji przedmiotu zamówienia, o którym mowa w ust.1, w terminie **dni** od dnia zawarcia umowy.
4. Wykonawca oświadcza, że dostarczone urządzenia serwerowe są fabrycznie nowe, wcześniej nie użytkowane, o parametrach technicznych zgodnych z parametrami określonymi w SWZ.

§ 2

1. Po dostarczeniu zamówionych urządzeń następuje ich przyjęcie przez Zamawiającego na podstawie protokołu zdawczo - odbiorczego. Przedstawiciel Wykonawcy upoważniony jest do obecności podczas tych czynności.
2. Wykonawca zobowiązuje się dostarczać Zamawiającemu wszelkie dokumenty dotyczące Sprzętu niezbędne do jego prawidłowej eksploatacji, sporządzone w języku polskim, w tym w szczególności instrukcję obsługi oraz dokumenty gwarancyjne Przedmiotu umowy niezbędne do zabezpieczenia Zamawiającego przed wszelkimi roszczeniami ze strony osób trzecich z tytułu naruszenia praw własności intelektualnej, w tym w szczególności praw autorskich, patentowych, praw ochronnych na znak towarowy, licencji nie później niż w dniu dostarczenia Zamawiającemu Przedmiotu umowy.
3. W razie zgłoszenia przez Zamawiającego uwag lub zastrzeżeń odnośnie funkcjonowania Przedmiotu umowy, Wykonawca zobowiązuje się, niezwłocznie, nie później jednakże niż w terminie 7 dni, do usunięcia wszelkich nieprawidłowości.
4. Osobami uprawnionymi do podpisania protokołu końcowego są:
 - ze strony Wykonawcy:
 - ze strony Zamawiającego: **Wojciech Bilski**
5. W razie zmiany danych osób uprawnionych do podpisania protokołu końcowego, wymienionych w ust. 4 niniejszego paragrafu każda ze stron zobowiązuje się powiadomić o tych zmianach drugą stronę na piśmie. Zmiana wywołuje skutek z chwilą poinformowania o niej drugiej strony.
6. Zamawiającemu przysługuje prawo odmowy przyjęcia dostarczonego Przedmiotu umowy i żądania wymiany na Sprzęt i wolny od wad w przypadku:
 - a) dostarczenia Przedmiotu umowy niewłaściwej jakości lub niezgodnego z właściwościami, które winien posiadać,
 - b) dostarczenia Przedmiotu umowy niezgodnego z zamówieniem.
7. Okres gwarancji wynosi:

Część I:

 - **Serwer 1 wraz z oprogramowaniem** – 60 miesięcy
 - **Macierz dyskowa** – 60 miesięcy
 - **Serwer 2 wraz z oprogramowaniem** – 60 miesięcyliczony od dnia realizacji tj. podpisania protokołu zdawczo - odbiorczego.

Część II

- **Urządzenie UTM** – do 30.06.2025 r.
8. W przypadku awarii sprzętu objętego gwarancją jego odbiór odbywa się przez Wykonawcę w siedzibie Zamawiającego po demontażu dysków twardych, który pozostaje w siedzibie Zamawiającego.
 9. W przypadku awarii dysku twardego, koszt jego wymiany ponosi Wykonawca w okresie gwarancji.
 10. Za dni robocze uznaje się dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz sobót. Za godziny pracy administracji uznaje się godziny od 7.30 do 15.00 w dni robocze.
 11. Zgłoszenie o awarii sprzętu przekazane przez Zamawiającego po godzinie 15 w danym dniu roboczym uznaje się za przekazane do serwisu o godzinie 7.30 pierwszego następnego dnia roboczego.

§ 3

1. Zgodnie ze złożoną ofertą wartość brutto przedmiotu umowy, o którym mowa w § 1 wynosi zł (słownie: złotych), zgodnie z formularzem ofertowym stanowiącym załącznik nr 1 SWZ.
2. Wartość przedmiotu umowy, o którym mowa w ust. 1, zawiera w sobie wszystkie koszty związane z realizacją przedmiotu umowy i stanowi ostateczną kwotę do zapłaty.
3. Należność, o której mowa w ust. 1, zostanie uregulowana przelewem z rachunku bankowego Zamawiającego na rachunek bankowy Wykonawcy wskazany na fakturze VAT, w terminie do 30 dni od daty dostarczenia prawidłowo wystawionej faktury z naliczonym na dzień wystawienia obowiązującym podatkiem VAT wraz z protokołem zdawczo-odbiorczym, o którym mowa w § 1 ust.2.
4. Strony postanawiają, że zapłata za przedmiot zamówienia następuje w dniu obciążenia rachunku bankowego Zamawiającego.

§ 4

1. Wykonawca zobowiązuje się do naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania.
2. W razie odstąpienia od umowy przez którąkolwiek ze stron w całości lub jej części z winy Wykonawcy, Wykonawca zapłaci karę w wysokości 10% wartości brutto całości lub tej części umowy, od której odstąpiono.
3. W razie zwłoki w realizacji przedmiotu umowy Wykonawca zapłaci karę umowną w wysokości 0,5% wartości brutto niezrealizowanej części dostawy, za każdy dzień zwłoki liczonej od dnia następnego po terminie, o którym mowa w §1 ust.3, nie więcej jednak niż 10% wartości brutto niezrealizowanej części dostawy. Niezależnie od naliczanych kar umownych Zamawiający zastrzega sobie prawo do odstąpienia od umowy w trybie natychmiastowym, jeżeli wykonanie przedmiotu umowy nie zostanie zrealizowane w terminie wskazanym w §1 ust.3.
4. Kary umowne, o których mowa w ust.2 i 3, podlegają w pierwszej kolejności potrąceniu z należności przysługującej Wykonawcy, a w przypadku braku możliwości potrącenia podlegają wpłacie na rachunek bankowy Zamawiającego.
5. W razie opóźnienia w zapłaceniu należności, o której mowa w §3 ust.1, liczonej od dnia następnego po upływie terminu określonego w §3 ust.3 umowy, Wykonawca może dochodzić odsetek ustawowych za opóźnienie w transakcjach handlowych, określonych w ustawie z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (Dz. U. z 2023 r. poz. 1790).
6. Limit kar umownych, jakich Zamawiający może żądać od wykonawcy z wszystkich tytułów przewidzianych w niniejszej umowie, wynosi 30% wartości brutto całości zamówienia określonej w §3 ust.1.
7. Strony mogą dochodzić na zasadach ogólnych odszkodowań przewyższających kary umowne.

§5

1. Żadna ze Stron Umowy nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy, spowodowane przez okoliczności traktowane jako siła wyższa. Przez siłę wyższą rozumie się zdarzenia pozostające poza

kontrolą każdej ze Stron, których nie mogły one przewidzieć ani zapobiec, a które zakłócają lub uniemożliwiają prawidłową realizację Umowy.

2. W przypadku zaistnienia siły wyższej Strona, której taka okoliczność uniemożliwia lub utrudnia prawidłowe wywiązanie się z jej zobowiązań, niezwłocznie, nie później jednak niż w ciągu 7 dni, powiadomi drugą Stronę o takich okolicznościach i ich przyczynie.
3. Jeżeli siła wyższa, będzie trwała nieprzerwanie przez okres 90 dni lub dłużej, Strony mogą w drodze wzajemnego uzgodnienia rozwiązać Umowę, bez nakładania na żadną ze Stron dalszych zobowiązań.
4. Okres występowania siły wyższej powoduje odpowiednie przesunięcie terminów określonych w Umowie.

§ 6

Ewentualne sprawy sporne, związane z wykonaniem przedmiotu umowy, podlegać będą postępowaniu polubownemu, a w przypadku braku konsensusu rozstrzygane będą przez sąd powszechny właściwy rzeczowo i miejscowo dla siedziby Zamawiającego.

§ 7

Wszelkie zmiany w treści umowy wymagają formy pisemnej pod rygorem nieważności.

§ 8

W sprawach nieuregulowanych niniejszą umową zastosowanie mają przepisy Kodeksu cywilnego (Dz. U. z 2024 poz.1061 z późn. zm.) oraz przepisy ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz.1320 z późn. zm.).

§ 9

Umowa wchodzi w życie z dniem podpisania przez ostatnią ze stron.

WYKONAWCA

ZAMAWIAJĄCY