ZNAK SPRAWY: RIR.271.35.2025

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego pn.:

Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd” w Gminie Dobrzyniewo Duże w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (DERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”

Zatwierdzono dnia: .....

Spis treści

I ZAMAWIAJĄCY

Gmina Dobrzyniewo Duże
ul. Białostocka 25
16-002 Dobrzyniewo Duże
NIP: 9661844107
REGON: 050659250
tel. 85 742 81 55

Niniejszy dokument określa minimalne wymagania dla zamówienia z zakresu cyberbezpieczeństwa w ramach realizacji projektu „Cyberbezpieczny Samorząd" dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa".
Postępowanie prowadzone jest zgodnie z postanowieniami ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (Dz. U. z 2024 r. poz. 1320) oraz aktów wykonawczych wydanych na jej podstawie.
Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy, a następnie Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji (art. 275 pkt 1 ustawy Pzp). Zamawiający nie przewiduje możliwości wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji (art. 275 pkt 2 ustawy Pzp).

Zamawiający w okresie 3 lat od dnia udzielenia zamówienia podstawowego, dotychczasowemu wykonawcy nie przewiduje udzielenia zamówienia polegającego na powtórzeniu podobnych usług.
Zamawiający nie dopuszcza składania ofert wariantowych.
Zamawiający nie przewiduje wymagań wskazanych w art. 96 ust. 2 pkt 2 ustawy Pzp.
Zamawiający nie przewiduje wymagań wskazanych w art. 94 ustawy Pzp.
Zamawiający nie przewiduje zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.
Zamawiający nie wymaga przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Pzp.
Zamawiający nie przewiduje rozliczenia między Zamawiającym a Wykonawcą w walutach obcych.
Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
Zamawiający nie wymaga obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań zgodnie z art. 60 i art. 121 ustawy Pzp.
Zamawiający nie przewiduje zawarcia umowy ramowej
Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230 ustawy Pzp.
Zamawiający nie stawia wymogu lub możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy Pzp.
Wykonawca jest związany ofertą do dnia **29.05.2025 r.** W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w SWZ, Zamawiający przed upływem terminu związania ofertą, zwróci się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni. Przedłużenie terminu związania ofertą, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
Zamawiający nie wymaga wniesienia wadium ani zabezpieczenia należytego wykonania umowy.
Wykonawca jest zobowiązany do wypełnienia obowiązku informacyjnego przewidzianego w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał (w przypadku korzystania z podwykonawców/ podmiotów trzecich/wykonawców wchodzących w skład konsorcjum) w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

II Definicje

Zamawiający dokonał opisu przedmiotu z wykorzystaniem następujących definicji:

Lp.	Termin	Definicje
1.	OPZ	Opis przedmiotu zamówienia
2.	Umowa	Należy przez to rozumieć umowę zawartą między zamawiającym a jednym lub większą liczbą wykonawców, której celem jest ustalenie warunków dotyczących zamówień, jakie mogą zostać udzielone w danym okresie, w szczególności cen i, jeżeli zachodzi taka potrzeba, przewidywanych ilości
3.	Zamawiający	Należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, obowiązaną na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych do jej stosowania.
4.	Wykonawca	należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą

		osobowości prawnej, która oferuje na rynku wykonanie robót budowlanych lub obiektu budowlanego, dostawę produktów lub świadczenie usług lub ubiega się o udzielenie zamówienia, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego.

III Wartość zamówienia

Szacunkowa wartość zamówienia nie przekracza wyrażoną w złotych równowartość kwoty określonej w przepisach wydanych na podstawie ustawy prawo zamówień publicznych z dnia 11 września 2019 r. (Dz. U. z 2024 r. poz. 1320).

IV Uzasadnienie braku podziału zamówienia na części

Zamówienie objęte niniejszym postępowaniem nie zostało podzielone na części. Zamawiający nie dopuszcza możliwości składania ofert częściowych w ramach przedmiotowego zamówienia.

Wartość zamówienia jest niższa od tzw. progów unijnych które zobowiązują do implementacji dyrektyw UE. Dyrektywa 2014/24/UE w treści motywu 78 wskazuje, że aby zwiększyć konkurencję, instytucje zamawiające powinny w szczególności zachęcać do dzielenia dużych zamówień na części. Przedmiotowe zamówienie nie jest dużym zamówieniem w rozumieniu motywu 78 powołanej dyrektywy UE (dyrektywy stosuje się od tzw. progów UE, a dyrektywa posługuje się pojęciem dużego zamówienia na gruncie zamówień podlegających dyrektywie, a więc zamówienia o wartości znacznie przewyższającej tzw. progi UE).

Należy podkreślić, że dostarczone oprogramowanie musi być kompatybilne z oferowanym sprzętem komputerowym oraz urządzeniami sieciowymi, w związku z tym zamawiający nie dokonał podziału zamówienia na części. Dzielenie zamówienia na części pod kątem ilości w efekcie przyniosłoby wzrost cen w stosunku do całkowitego zakresu zamówienia, ze względu na konieczność odrębnego wliczania kosztów pośrednich przez każdego ze startujących wykonawców (np. koszty ubezpieczenia, transportu, koordynatorów, systemu utrzymania gwarancji). Niniejsze zamówienie dotyczy zakresu o zasięgu, który sprawia, iż wykonanie go w ramach jednej części i przez jednego wykonawcę będzie stanowić najbardziej efektywny z punktu widzenia technicznego i formalnego sposób realizacji. Zamawiający otrzyma również gwarancję na dostarczony przedmiot zamówienia od jednego wykonawcy, a w przypadku większej liczby wykonawców mogłyby wystąpić duże problemy z wyegzekwowaniem roszczeń. Zastosowany ewentualnie podział zamówienia na części nie zwiększyłby konkurencyjności w sektorze małych i średnich przedsiębiorstw – zakres zamówienia jest zakresem typowym, umożliwiającym złożenie oferty wykonawcom z grupy małych lub średnich przedsiębiorstw. Zgodnie z treścią motywu 78 dyrektywy, Instytucja zamawiająca powinna mieć obowiązek rozważenia celowości podziału zamówień na części, jednocześnie zachowując swobodę autonomicznego podejmowania decyzji na każdej podstawie, jaką uzna za stosowną, nie podlegając nadzorowi administracyjnemu ani sądowemu.

Reasumując, zamawiający nie dokonał podziału zamówienia na części ze względu na to, że podział taki groziłby nadmiernymi trudnościami technicznymi oraz nadmiernymi kosztami wykonania zamówienia. Niedokonanie podziału zamówienia podyktowane było zatem względami ekonomicznymi, technicznymi, organizacyjnym oraz charakterem przedmiotu zamówienia.

Ponadto, istnieje ryzyko, że w przypadku podzielenia zamówienia na części, na którąś z nich mogłaby nie zostać złożona żadna oferta wykonawcy, co skutkowałoby tym, iż dany zakres mógłby nie zostać zrealizowany.

Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 8.

V Opis przedmiotu zamówienia

1. Serwer do wykonywania kopii zapasowych – 1 szt.

Obudowa

- Typu RACK, wysokość 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy;
- Możliwość zainstalowania 16 dysków twardych hot plug 2,5”;
- Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD SATA 12G 960GB 2,5” Hot-Plug o DWPD min.5 skonfigurowane w RAID 1, przyłączone do sprzętowego kontrolera z obsługą do 16 dysków;
- Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;
- Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
- Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-9.

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Zainstalowany moduł TPM 2.0;
- 6 złącz PCI Express generacji 5 w tym:
  - 4 fizyczne złącza o prędkości x16;
  - 2 fizyczne złącza o prędkości x8;
  - Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
  - Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
- 32 gniazda pamięci RAM;
- Obsługa minimum 8 TB pamięci RAM;
- Wsparcie dla technologii:
  - Memory Scrubbing;
  - SDDC;
  - ECC;
  - Memory Mirroring;
  - ADDDC;
- Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.

Procesory

- Minimum Dwa procesory osiągające w teście SPECrate2017_int_base wynik min. 172pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html na dzień składania ofert

Pamięć RAM

- Min. 256 GB pamięci RAM;

Kontrolery LAN, nie zajmujące żadnego z dostępnych slotów PCI Express;

Interfejsy LAN,:

- 2x 10Gbit Base-T
- 1x 1Gbit Base-T
- Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Interfejsy LAN i SAN zainstalowane w slotach PCI-e:

- 2x 10Gbit Base-T
- 2x FC 32Gb

Kontrolery I/O

- Kontroler SAS RAID dla dysków wewnętrznych, 8 GB pamięci cache z mechanizmem podtrzymania, obsługujący poziomy RAID: 0, 1, 10, 5, 50, 6, 60
- Kontroler SAS w postaci karty PCIe min. 2 portowy SAS do obsługi biblioteki taśmowej, interfejs karty x8 PCIe 4.0, obsługa 12/6 Gb/s SAS

Porty

- Zintegrowana karta graficzna ze złączem VGA z tyłu, możliwe opcjonalnie złącze VGA z przodu serwera;
- 1 port USB 3.0 wewnętrzny;
- 2 porty USB 3.0 dostępne z tyłu serwera;
- 2 porty USB 3.0 na panelu przednim;
- Możliwy opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
- 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 900W;
- Redundantne wentylatory hotplug.

Zarządzanie

- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
    - informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
        - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
        - procesory CPU;
        - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
        - status karty zarządzającej serwera;
        - wentylatory;
        - bateria podtrzymująca ustawienia BIOS płyty głównej;
        - zasilacze;
        - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);

- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
    - Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
    - Dedykowana karta LAN 1 Gb/s oraz dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
    - Dostęp poprzez przeglądarkę Web, SSH;
    - Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
    - Zarządzanie alarmami (zdarzenia poprzez SNMP);
    - Możliwość przejęcia konsoli tekstowej;
    - Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
    - Obsługa serwerów proxy (autentykacja);
    - Obsługa VLAN;
    - Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
    - Wsparcie dla protokołu SSDP;
    - Obsługa protokołów TLS 1.2, SSL v3;
    - Obsługa protokołu LDAP;
    - Integracja z HP SIM;
    - Synchronizacja czasu poprzez protokół NTP;
    - Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o wielkości min. 128 GB dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Serwer powinien posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

- Microsoft Windows Server 2022, 2019;
- VMWare vSphere 8.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9, 8;
- Microsoft Hyper-V Server 2019.

Gwarancja

- min. 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
- Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
- Zgodność z normami: CB, RoHS, WEEE oraz CE.

Wraz z serwerem należy dostarczyć licencję Microsoft Windows Server 2025 x64 Standard PL lub produkt równoważny. Za równoważność rozumie się zakup produktu obejmującego licencję systemu operacyjnego który zapewnia:
- licencję obejmującą minimum 16 rdzeni procesora(ów),
- Obsługę Server Containers.
- Możliwość pełnienia funkcji drugiego kontrolera domeny Active Directory
w istniejącej infrastrukturze Zamawiającego (zgodność z AD na poziomie Windows Server 2022)
-możliwość aktualizacji w tle utrzymując ciągłość działania nawet podczas wdrażania poprawek.
- interfejsy użytkownika dostępne w wielu językach do wyboru - w tym polskim i angielskim,
- graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
- wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
- zabezpieczenie hasłem dostępu do systemu, konta i profilu użytkowników,
- mechanizmy logowania w oparciu o login i hasło,
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości współbieżnej (ang. Simultaneous Multi-Threading, SMT).
- Wbudowane wsparcie instalacji i pracy na wolumenach, które:
a) pozwalają na zmianę rozmiaru w czasie pracy systemu
b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu
dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

- Wsparcie dla środowisk Java i .NET Framework 6.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych
producentów wymagających dodatkowych licencji:
a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe).
c) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 2 aktywnych środowisk wirtualnych systemów operacyjnych.
- Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
Dostarczone oprogramowanie musi być fabrycznie nowe.

2. Macierz dyskowa – 1 szt.

Lp.	Nazwa elementu, parametru lub cechy	Szczegółowy opis wymagań
1.	Obudowa – gęstość upakowania	Macierz musi umożliwiać instalację w standardowej szafie RACK 19”.
2.	Obudowa – gęstość upakowania	Macierz musi mieć możliwość instalacji kombinacji poniższych nośników dyskowych w ramach jednej obudowy podstawowej (zawierającej kontrolery): - Flash NVMe lub NVMe SSD, gdzie Flash NVMe oznacza dyski autorskie dostawców macierzy wykorzystujące protokół NVMe - SCM (Storage Class Memory)
3.	Obudowa – gęstość upakowania	Możliwość zainstalowania co najmniej 12 dysków NVMe o rozmiarze 2,5” cala w obudowie o wysokości 1U.
4.	Obudowa – gęstość upakowania	Kontrolery macierzowe muszą komunikować się z nośnikami dyskowymi umieszczonymi w obudowie podstawowej (zawierającej kontrolery) wyłącznie z użyciem protokołu NVMe.
5.	Obudowa – gęstość upakowania	Macierz musi być zbudowana z minimum dwóch kontrolerów pracujących w trybie active-active lub dual-active.
6.	Obudowa – gęstość upakowania	Architektura macierzy ma być oparta o sprawdzone i powszechnie dostępne procesory technologii x86/x64
7.	Funkcje niezawodnościowe	Wszystkie krytyczne komponenty macierzy takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienialne w trakcie pracy macierzy.
8.	Funkcje niezawodnościowe	Macierz musi cechować brak pojedynczego punktu awarii.

9.	Funkcje niezawodnościowe	Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. Wentylatory typu Hot-Swap.
10.	Zarządzanie	Macierz musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej.
11.	Zarządzanie	Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
12.	Zarządzanie	Urządzenie musi składać się z pojedynczej macierzy dyskowej zarządzanej z jednego wbudowanego w macierz interfejsu GUI (interfejs graficzny), CLI (interfejs tekstowy) oraz zapewniać możliwość tworzenia skryptów użytkownika. Interfejs ten musi być natywnie dostępny na macierzy, bez zastosowania zewnętrznych urządzeń.
13.	Ilość portów	Wymagane jest nie mniej niż 4 x FC 32Gb/s per kontroler
14.	Pojemność użytkowa	Całkowita pojemność min. 15 TiB netto (użyteczne przy założeniu konfiguracji odpornej na awarię minimum 2 dysków (typu RAID-6 lub równoważnego) oraz bez uwzględnienia technik redukcji danych takich jak kompresja, deduplikacja czy thin-provisioning) i musi być zbudowana wyłącznie w oparciu o nośniki NVMe Flash lub NVMe SSD.
15.	Pojemność użytkowa	Macierz musi pozwalać na alokację 99% pojemności użytecznej bez spadku wydajności macierzy (brak zwiększonego czasu odpowiedzi, brak spadku przepustowości macierzy). Wydajność macierzy musi być niezależna od poziomu alokacji przestrzeni macierzy w zakresie od 0% alokacji do wartości wymaganej pojemności użytecznej. Jeżeli oferowane rozwiązanie nie spełnia opisanego wymagania należy dostarczyć co najmniej 20% pojemności użytecznej więcej.
16.	Obsługiwane poziomy RAID	Macierz musi obsługiwać poziomy: RAID1, RAID5 i RAID6 (dystrybuowane) i zapewniać zabezpieczenie przed awarią dwóch dysków jednocześnie w ramach jednej grupy raid.
17.	Bezpieczeństwo danych	Dyski/przestrzeń "spare" muszą zostać skonfigurowane/dostarczone w ilości/pojemności zgodnej z udokumentowanymi rekomendacjami producenta oferowanej macierzy. Macierz musi posiadać wbudowane sprzętowo na nośnikach dyskowych NVMe szyfrowanie AES-256. Kontrolery macierzowe muszą posiadać możliwość szyfrowania danych, uniemożliwiając odczyt danych z usuniętych z macierzy nośników dyskowych. Ta funkcjonalność nie jest to objęta tym postępowaniem.
18.	Skalowalność rozwiązania	Macierz musi mieć możliwość obsługi min. 200 dysków poprzez dodanie półek rozszerzeń. Macierz musi mieć możliwość rozbudowy poprzez dodanie pojedynczego dysku, dodanie kontrolerów oraz półek dyskowych.

19.	Skalowalność rozwiązania	Niezależnie od zastosowanych nośników danych, macierz musi umożliwiać granularną rozbudowę grupy RAID w zakresie od co najmniej od 1 do 12 nośników dyskowych, proces rozbudowy nie może powodować niedostępności do danych.
20.	Kontrolery macierzy dyskowej	Macierz musi być wyposażona w minimum 2 kontrolery dyskowe z możliwością rozbudowy do 4 kontrolerów. Każdy z kontrolerów musi udostępniać co najmniej 120GB pamięci Cache.
21.	Kontrolery macierzy dyskowej	Macierz musi umożliwiać rozbudowę pamięci cache do 1TB w ramach klastra macierzy składającego się z identycznych kontrolerów i zarządzanego z jednego interfejsu GUI, CLI. Zamawiający nie dopuszcza zastosowania dysków SSD/ SSD NVMe lub kart pamięci/modułów FLASH jako rozszerzenia pamięci cache.
22.	Funkcjonalności	Funkcjonalność partycjonowania pamięci cache.
23.	Funkcjonalności	Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami.
24.	Funkcjonalności	Funkcjonalność dynamicznego zwiększania rozmiaru wolumenów.
25.	Funkcjonalności	Funkcjonalność zarządzania maksymalną ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie - zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s.
26.	Funkcjonalności	Macierz musi mieć możliwość kompresji i deduplikacji dla wszystkich rodzajów dysków. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową Wsparcie dla kompresji danych w trybie inline („na bieżąco” bez potrzeby zapisywania danych na nośnikach danych w formie nie skompresowanej) dla dostępu blokowego.
27.	Technologia optymalizacji przestrzeni zajmowanej przez dane	Macierz musi wspierać kompresję i deduplikację w trybie "inline".
28.	Wysoka dostępność	Zaoferowane rozwiązanie musi posiadać możliwość implementacji klastra wysokiej dostępności. W ramach architektury klastra wysokiej dostępności musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednej z macierzy nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana niezależnie od systemu operacyjnego na poziomie przełączania ścieżek do urządzenia logicznego. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.
29.	Optymalizacja wykorzystania zasobów wewnętrznych	Macierz musi optymalizować wykorzystanie dysków SSD/ modułów Flash/ HDD, tak aby w ramach tego samego rodzaju dysków (pojemności/prędkości) wszystkie grupy dysków były utylizowane w

		równym stopniu. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy.
30.	Obsługa wirtualnych dysków logicznych	Macierz musi mieć możliwość rozłożenia wolumenu logicznego pomiędzy co najmniej dwoma różnymi typami macierzy dyskowych
31.	Obsługa wirtualnych dysków logicznych	Macierz musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi macierzami, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta.
32.	Funkcjonalność thin provisioning	Macierz musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność macierzy.
33.	Kopie migawkowe	Kopie danych typu snapshot (PIT) muszą być tworzone w trybach incremental, multitarget, oraz kopii pełnej oraz kopii wskaźników. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy.
34.	Kopie migawkowe	Macierz musi posiadać możliwość tworzenia kopii migawkowych w trybie WORM (Write Once Read Many). Kopie powinny być tworzone za pomocą harmonogramu i mieć możliwość ustawienia retencji kopii, po upłynięciu której kopia automatycznie zostanie usunięta z macierzy.
35.	Replikacja danych pomiędzy macierzami	Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA). Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.
36.	Inne	Macierz musi być nowa, nigdy wcześniej nie używana i pochodzić z autoryzowanego kanału dystrybucji producenta a także być objęta serwisem producenta na terenie RP.
37.	Wsparcie systemów operacyjnych	Wsparcie systemów operacyjnych Macierz musi być wspierana przez systemy operacyjne i wirtualizatory: MS Windows Server 2019, 2022, Vmware vSphere 7 i nowsze, RedHat Enterprise Server 7.9 i nowsze
38.	Integracja z rozwiązaniem backupu	Macierz musi zapewniać integrację z oprogramowaniem spełniającym wymogi opisane w punkcie 6. Dotyczy opisu oprogramowania do backupu

39.	Gwarancja	Wymagana jest gwarancja świadczona w trybie 24 godziny przez 7 dni w tygodniu, z czasem reakcji w tym samym dniu roboczym od zgłoszenia awarii, na wszystkie elementy macierzy (sprzęt oraz oprogramowanie) na okres min. 36 miesięcy. Uszkodzone dyski pozostają własnością Zamawiającego. Usługi serwisowe będą świadczone przez producenta oferowanego sprzętu lub autoryzowanym serwisem

3. Karta SAN FC do serwerów Fujitsu PY RX2540 M6 – 3 szt.

LP	Parametr lub warunek	Minimalne wymagania
1	Wysokość	Karta uniwersalna o wysokości FH/LP
2	Liczba i rodzaj interfejsów	2x min.32Gb/s FC LC
3	Złącze PCIe	PCIe 4.0 x8
4	Zgodność	Certyfikowana do pracy w serwerze Fujitsu PY RX2540 M6/M7
5	Gwarancja	Min. 3 lata gwarancji producenta serwera

4. Serwer do wykonywania kopii zapasowych z oprogramowaniem do wirtualizacji – 1 szt.

Lp.	Elementy	Wymagane parametry i właściwości urządzenia
1.	Wykorzystana technologia	LTO-9 wspierające technologię partycjonowania nośników. Urządzenie musi mieć możliwość instalowania w tej samej obudowie także napędów LTO innych generacji
2.	Wbudowane napędy	Minimum jeden napęd LTO-9 wyposażony w złącze z interfejsem dual SAS 12Gb/s. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie także napędów LTO9 z interfejsem dual FC 8Gb/s oraz wspierać technologię LTFS (Linear Tape File System) kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu LTO-9 bez kompresji – do 300 MB/sek. Zainstalowany napęd powinien mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) oraz stosować szyfrowanie danych metodą AES 256-bit
3.	Ilość slotów i magazynki	Minimum 8 kieszeni na taśmy (urządzenie musi być dostarczone z kompletem magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot powinna odbywać się bez konieczności wysuwania całego magazynka.
4.	Pojemność	Pojemność bez kompresji – minimum 144TB
5.	Obudowa	Typu rack 19”. Wszystkie elementy do montażu winny być dostarczone wraz z urządzeniem, wysokość maksymalnie 1U
6.	Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą

		interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 3 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI. Aktualizacja firmware robota biblioteki oraz napędu musi być możliwa poprzez web GUI oraz USB (panel operatora).
7.	Dodatkowe interfejsy	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI
8.	Obsługa urządzenia	Wymagana możliwość wymiany napędu, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i moduł portów zarządzania powinny być wyposażone w lampki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki.
9.	Partycjonowanie	Wymagana jest możliwość stworzenia 1 logicznej partycji na urządzeniu – jeżeli do tej operacji konieczna jest dodatkowa licencja, należy ją dostarczyć wraz z urządzeniem.
10.	Wyposażenie	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli koniecznych do podłączenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabli min. 2m. Wraz z urządzeniem należy dostarczyć także zestaw nośników danych o pojemności bez kompresji minimum 18,0 TB każdy w ilości 20 szt. oraz 2 nośniki czyszczące, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, wszystkie nośniki muszą być wyposażone w etykiety z kodami kreskowymi i możliwością zastosowania logo użytkownika. Instrukcja instalacji - w języku polskim lub angielskim
11.	Gwarancja i oświadczenia	min. 36 miesięcy w serwisie szybkiej wymiany komponentu w przypadku awarii, w którym to wymienny komponent wysyłany jest awansem do użytkownika a użytkownik zwraca uszkodzony. Czas reakcji na zgłoszenia do następnego dnia roboczego. Czas przyjmowania zgłoszeń serwisowych w trybie 5x9. Przystąpienie do procesu wymiany najpóźniej w następnym dniu roboczym od zdiagnozowania awarii z terminem wysyłki najpóźniej do 48 godzin od zdiagnozowania usterki. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 72 miesięcy. Wsparcie i gwarancja muszą obejmować zarówna samo urządzenie jak i wszystkie zainstalowane w nim napędy oraz dostarczone nośniki. Zgłaszanie awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta – kontakt z serwisem w języku polskim. Autoryzowany serwis producenta posiadający aktualne certyfikaty ISO9001, ISO14001, ISO27001, AQUAP 2110 lub równoważne obejmujące usługi serwisowe oferowanego urządzenia Możliwości przedłużenia gwarancji do 72 miesięcy. Dostarczone urządzenie musi być fabrycznie nowe, nie używane, wyprodukowane nie wcześniej niż rok od składania oferty oraz pochodzić z autoryzowanego kanału sprzedaży producenta na terenie Polski. Oferowane urządzenie zgodne z europejskimi normami dotyczącymi CE i WEEE

5. Serwer NAS – 1 szt.

Lp.	Nazwa elementu, parametru lub cechy	Szczegółowy opis wymagań
1.	Procesor	Procesor musi osiągać wynik co najmniej 34000 punktów w teście porównawczym znajdującym się na stronie https://www.cpubenchmark.net/
2.	Obudowa	Rack 2U o wymiarach maksymalnych 89 × 482 × 550 mm (wys. x szer. x gł.) wraz z szynami do montażu w szafie rack
3.	Pamięć RAM	32 GB Możliwość rozbudowy poprzez dołożenie kolejnych pamięci do min. 192 GB (4 x 48GB)
4.	Ilość obsługiwanych dysków	12 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s o maksymalnej pojemności 24TB każdy
5.	Gniazda m.2	2 gniazda M.2 2280 PCIe Gen 5
6.	Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (RJ45) 2 porty 10GbE (10GBase-T) możliwość zamontowania (jako płatna opcja): - dodatkowej karty sieciowej 100GbE, - dodatkowej karty sieciowej FC 16GbE, - dodatkowej karty sieciowej FC 32GbE, - obsługa VLAN i Jumbo Frame.
7.	Porty USB	Minimum 2 gniazdo typu A USB 3.2 Gen 2 10 Gb/s
8.	Porty PCIe	Minimum 3 gniazda PCIe 2 x Gen 4 x4, 1 x Gen 4x8 (lub Gen 4x4)
9.	Wskaźniki LED	HDD 1–12, stan, LAN, stan gniazda rozszerzenia pamięci masowej
10.	Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.
11.	Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.
12.	Szyfrowanie	256-bitowe szyfrowanie AES folderów
13.	System Operacyjny	Apple Mac OS 10.10 lub nowszy Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux IBM AIX 7, Solaris 10 lub nowszy UNIX Microsoft Windows 7, 8, 10, 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019 oraz 2022
14.	Wirtualizacja	Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android Import maszyn wirtualnych Klonowanie maszyn wirtualnych Migawki maszyn wirtualnych GPU pass-through dla dodatkowych kart graficznych
15.	Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
16.	Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog
17.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
18.	Język GUI	Polski

19.	Gwarancja producenta	min. 36 miesięcy gwarancji Producenta sprzętu
20.	Waga	Maksymalnie 14 kg (netto)
21.	System plików	Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
22.	Funkcje ZFS	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
23.	iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
24.	Liczba kont użytkowników	4096
25.	Liczba grup	512
26.	Liczba udziałów	512
27.	Max ilość połączeń (CIFS)	5000
28.	Zasilanie	Redundantne 550W (x2), 100–240 V
29.	Wentylatory	3 x 60mm, 12VDC
30.	UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.
31.	Zamontowane dyski	12 dysków o pojemności minimum 8TB każdy, 256MB cache, 7200RPM, 2 mln MTBF, gwarancja producenta 5 lat, zgodnych z listą kompatybilną podaną przez producenta NAS o parametrach minimalny transfer wewnętrzny 255MB/sek

6. Licencja na oprogramowanie do zabezpieczenia danych – 1 kpl. - Oprogramowanie do wykonywania kopii zapasowych

Licencje na oprogramowanie do zabezpieczania danych min. 20 maszyn wirtualnych, licencje wieczyste, 1 rok wsparcia, licencje spełniające poniższe wymagania minimalne:

Wymagania ogólne
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk typu DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions
Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Całkowite koszty posiadania
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
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 musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych do takiej puli.
Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS)
Oprogramowanie musi posiadać integracje z systemami typu SIEM

Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
Wymagania RPO
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
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 z dokładnością do pojedynczego datastoru
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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 mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka
Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Środowiska fizyczne
Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych

Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
Rozwiązanie musi wspierać system operacyjny macOS
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
Rozwiązanie musi wspierać backup podłączonych dysków USB
Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
Rozwiązanie musi wspierać kontrolę pasma sieciowego
Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
Rozwiązanie musi wspierać technologię BitLocker
Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
Rozwiązanie musi wspierać szyfrowanie
Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Monitoring
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 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby

otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
Raportowanie
System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

7. System bezpieczeństwa sieciowego typ 1 – szt. 1

Wymagania Ogólne

Urządzenie musi mieć możliwość połączenia w tzw. Security Fabric z wykorzystywanymi przez zamawiającego urządzeniami Fortigate FG-70F w celu centralnego zarządzania urządzeniami.
System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. 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.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

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

Ochrona przed atakami

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

Kontrola aplikacji

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

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. 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.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Testy wydajnościowe oraz funkcjonalne

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

Serwisy i licencje

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

a) 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 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

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

8. Zarządzalne urządzenia sieciowe z obsługą VLAN – 2 szt.

1. Rodzaj i liczba portów
   - Typ i liczba portów: - 12x 10Gigabit Ethernet SFP+, 12x 10Gigabit Ethernet RJ45, 1xGigabit Ethernet
   - Obudowa 1U, rackmount (dostarczone uchwyty montażowe)
   - Możliwość stackowania przełączników w ramach jednolitej rodziny przełączników – do min. 160 portów 10 Gigabit Ethernet w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym Link Aggregation i port mirroring
2. Zarządzenie energią:
   - Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)
   - Możliwość wyłączenia diod LED w celu oszczędzania energii

3. Parametry wydajnościowe:
    - Przełącznik line-rate zapewniający pracę z pełną wydajnością wszystkich interfejsów
    - Pamięć DRAM – 1GB
    - Pamięć Flash – 512MB
    - Wielkość bufora pakietów – 8 MB
    - Obsługa 4000 sieci VLAN
    - 16.000 adresów MAC
    - Wire-speed IPv4 routing – 990 tras statycznych; 128 interfejsów IP
    - Obsługa ramek jumbo – do 9000 bajtów
    - 2000 IGMP group
    - 8 połączeń zagregowanych typu „port channel”
    - Ilość wpisów w listach kontroli dostępu Security ACL – 1000
    - Wydajność przełączania pakietów: min. 357 mln pakietów na sekundę (pakiety 64B)
    - Wydajność przełączania 480Gbps
4. Obsługa protokołu SNTP
5. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
6. Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    - IEEE 802.1w Rapid Spanning Tree
    - IEEE 802.1s Multi-Instance Spanning Tree
    - Per-VLAN Rapid Spanning Tree (PVRST+)
    - Obsługa 126 instancji protokołu STP
8. Obsługa protokołu LLDP i LLDP-MED
9. Obsługa Q-in-Q oraz Selective Q-in-Q
10. Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)
11. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
12. Możliwość uruchomienia funkcji serwera DHCP
13. Mechanizmy związane z bezpieczeństwem sieci:
    - Wiele poziomów dostępu administracyjnego poprzez konsolę
    - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    - Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard
    - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
    - Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community
    - Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priorty, TCP flag. Obsługa czasowych list ACL
    - Obsługa mechanizmów zapewaniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]

- Bezpieczny proces bootowania urządzenia
- Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika

14. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    - Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
    - Kontrola sztormów dla ruchu broadcast/multicast/unicast
    - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
    - Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu
15. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN z możliwością konfiguracji do 4 sesji monitorujących
16. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
17. Obsługa protokołu sFlow
18. Zarządzanie:
    - Port konsoli – USB typu C i RJ45
    - Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia
    - Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP
    - Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami
    - Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
    - Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu
19. Zasilacz AC 230V
20. Praca w szerokim zakresie temperatur: -5^{o}C – 50^{o}C
21. Głębokość urządzenia nie więcej niż 35cm.
22. Razem z przełącznikami należy dostarczyć sumarycznie następujące kompatybilne akcesoria:
    - kabel DAC 10Gb SFP+ 1m – 2 szt.
    - Moduł optyczny SFP+ LR 10Gbs 1310nm LC DDM SMF min. 10km – 12 szt.
    - Patch cord SC/APC-LC/UPC, SM, Duplex, długość 3m – 12 szt.
23. Gwarancja
    - Urządzenia muszą być objęte gwarancją producenta na okres min. 60 miesięcy oraz wsparciem przez pierwsze 90 dni od zakupu;
    - Zamawiający wymaga, by dostarczone urządzenia były fabrycznie nowe, wyprodukowane nie dawniej niż na 12 miesięcy przed ich dostarczeniem; urządzenia muszą pochodzić z oficjalnego i autoryzowanego kanału sprzedaży producenta urządzenia. Zamawiający zastrzega sobie możliwość weryfikacji numerów seryjnych dostarczonego urządzenia u Producenta w celu sprawdzenia czy urządzenie pochodzi z legalnego kanału sprzedaży;

- Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży (End Of Life, End Of Sale);
- Zamawiający wymaga aby zapewniony był dostęp do minimum aktualizacji krytycznych, oprogramowania przez cały okres obowiązywania gwarancji;
- Zamawiający nie dopuszcza składania ofert zawierających sprzęt poserwisowy lub refabrykowany.

9. Przełącznik sieciowy z PoE – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Typ	Przełącznik sieciowy Ethernet Smart Management rack 1Gbit.
2.	Porty	a) Minimum 24 porty 1G RJ45 10/100/1000BASE-T z czego 20 portów wspiera funkcję PoE+ 802.3at oraz 4 porty PoE+ 60W 802.3bt b) Minimum 2 porty SFP+ z możliwością pracy 1G/10G c) Minimum 2 porty 10GBASE-T (miedziane) Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX
3.	Parametry fizyczne	Wysokość maksymalnie 1U, montowany w szafie typu rack 19''
4.	Pamięć	Co najmniej 1GB Co najmniej 512MB Bufor pakietów minimum 1.5 MB
5.	Wielkość tablicy adresów MAC	Co najmniej 16000
6.	Ilość obsługiwanych sieci VLAN	Co najmniej 512
7.	Wydajność	• Przepustowość przełączania: min. 128 Gbit/s • Przełączanie dla pakietów: min. 95 Mpps. • Opóźnienie: < 4.4 uSec dla 100 Mb < 2.2 uSec dla 1000 Mb < 1.1 uSec dla 10 Gbps
8.	Obsługa ramek Jumbo	O wielkości co najmniej 9216 bajtów

9.	Funkcjonalność urządzenia	• obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad), • obsługa protokołu SNTP, • Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s) • Automatyczne przydzielanie klasy urządzenia PoE w oparciu o LLDP oraz LLDP-MED. • Minimum 100 możliwych do utworzenia ACL ingres oraz minimum 960 ACE, • CoS zgodna z 802.1p minimum 8 kolejek) • Kolejkowanie zgodne z Strict Priority lub Weighted Round Robin • Voice VLAN • Minimum 509 wpisów ARP • Możliwość przechowywania dwóch obrazów oprogramowania: aktywny I zapasowy • Port Security • DHCP Snooping • Klient Radius • Możliwość łączenia z minimum 4 serwerami Radius • Port mirroring, • DHCP Relay, • DoS Protection, • SNMP v1/v2c/v3 • ARP Attack Protection, • Możliwość utworzenia minimum 32 statycznych wpisów IPv4 w tablicy routingu • Możliwość utworzenia stosu w topologii pierścień lub łańcuch za pośrednictwem portów uplinkowych, składającego się z maksymalnie 4 urządzeń tej samej rodziny i zarządzania nimi z poziomu jednego adresu IP
10.	Zasilanie	Zasilacz 230V AC wbudowany, przystosowany do pracy z zakresami napięć: 100-127VAC oraz 200-240VAC
11.	Temperatura pracy	0°C do 40°C
12.	Maksymalny pobór mocy	100-127V: 500W 200-220V: 480W
13.	Zarządzanie	WWW (GUI), SNMP Manager, cloud-based web portal
14.	Gwarancja	Ograniczona gwarancja dożywotnia, obowiązuje tak długo, jak produkt jest używany przez pierwszego właściciela, dodatkowo jest ograniczona do pięciu (5) lat od daty wycofania przez producenta produktu ze sprzedaży. W ramach gwarancji produkty są objęte 90-dniowym całodobowym telefonicznym wsparciem technicznym. Przez pozostały okres gwarancji, dostępne wsparcie techniczne za pomocą czatu. Bezpłatny dostęp do wersji oprogramowania i jego aktualizacji przez cały okres posiadania urządzenia, dotyczy wszystkich ogólnodostępnych wersji oprogramowania / systemów operacyjnych.
15.	Dokumenty, certyfikaty	Deklaracja zgodności CE oferowanego urządzenia

10. UPS – 1 szt.

Oferowane urządzenie do bezprzerwowego zasilania musi być fabrycznie nowe i pochodzić z seryjnej produkcji. Producent oferowanego urządzenia powinien posiadać własny certyfikat ISO 9001 oraz 14001 jako potwierdzenie wymagań międzynarodowego standardu jakości. Oferowane urządzenie musi posiadać oznakowanie CE.
UPS musi spełniać poniżej opisane wymagania - nie gorsze niż:

1. Moc wyjściowa UPS 2 kVA / 1,8 kW

2. UPS przystosowany do instalacji jako Tower.
3. Zakres napięcia wejściowego: 160 – 285V AC
4. Zakres dopuszczalnej częstotliwości wejściowej: 40 – 70Hz
5. Współczynnik mocy wejściowy: >0,99
6. Wyjściowy współczynnik mocy równy: 0,9
7. THDu ≤ 3 %
8. Regulacja napięcia wyjściowego: ± 1%
9. Dopuszczalne przeciążenie: < 105% praca ciągła; 106 – 110%: 10 min; 111 – 130%: 30 sek; 131-150%: 30 sek.
10. Ilość gniazd wyjściowych IEC C13 – 4szt.
11. Urządzenie musi zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i wahaniach częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia.
12. Urządzenie powinno być wyposażone diody LED oraz w komunikacyjny wyświetlacz LCD z odczytem parametrów elektrycznych wejścia/wyjścia i komunikatów o stanie pracy UPS
    - Tryb Online
    - Tryb ECO
    - Tryb Bateryjny
    - Tryb konwersji częstotliwości
    - Napięcie wejściowe
    - Napięcie wyjściowe
    - Pojemność baterii
    - Czas podtrzymania
    - Wartość online XkVA
13. Preferowany kolor obudowy: czarny.
14. Poziom hałasu urządzenia w trybie podwójnego przetwarzania przy obciążeniu znamionowym nie może przekraczać 45 dB.
15. Sprawność w trybie TRUE ONLINE
    - do 90% w trybie normalnym
    - do 95% osiągane w ekonomicznym trybie pracy
16. UPS musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:
    - Gniazda umożliwiającej instalacje karty SNMP z obsługą protokolu SNMP v1/v3 /Relay/Modbus
    - USB
    - Gniazdo komunikacji RS-232
17. Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną:
    - Windows XP – SP2, Vista, Win7, 8 &10.
    - Windows 2003/2008.
    - Windows 2008 Server Core, Hyper-V 2008 R2.
    - Linux Opens USE 11.4, ubuntu 10.04, Fedora 3.1.9.
    - CentOS 5.8
    - Citrix XenServer 6.0.0.
    - Linux KVMLinux KVM
    - VMWare ESXi 4.1, 5

Gwarancja, warunki dostawy i sposób serwisowania

1. Gwarancja producenta min. 60 miesięcy na urządzenie oraz min. 36 miesięcy na akumulatory.
2. Producent zapewnia dostępność części zamiennych przez co najmniej 10 lat.
3. Producent posiada na terenie Europy:
   - centrum serwisowe
   - centrum testowe

11. Licencje oprogramowania sieciowego systemu operacyjnego systemu - 3 szt.

Licencje Windows Server 2025 Datacenter na 2 serwery wyposażone w jeden procesor 16-rdzeniowy oraz jeden serwer posiadający dwa procesory 12 rdzeniowe, licencje bezterminowe, przenaszalne

lub licencje równoważne spełniające poniższe funkcjonalności:

Lp.	Parametry, funkcjonalności
1.	Oprogramowanie systemowe przeznaczone do uruchamiania środowiska wirtualizacji oraz wirtualnych systemów operacyjnych usług serwerowych dla użytkowników w sieci lokalnej oraz Internetu.
2.	Możliwość instalowania aktualizacji zabezpieczeń systemu operacyjnego w systemie bez konieczności ponownego uruchamiania maszyny tzw. hotpatching.
3.	Usługi zintegrowane dostępne w systemie: Serwer usług katalogowych LDAP, ActiveDirectory, serwer plików i drukarek dla systemów Windows, serwer uwierzytelniania typu RADIUS dla użytkowników lokalnej sieci bezprzewodowej, usługi pojedynczego logowania typu SingleSignOn dla użytkowników komputerów lokalnych, drukarek sieciowych, serwer WWW, podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. Aplikacje zewnętrzne możliwe do instalacji w systemie: systemy baz danych typu MSSQL i Oracle, inne aplikacje lokalne i internetowe wykonane z użyciem technologii .NET i COM
4.	Zarządzanie centralne zasobami lokalnej sieci komputerowej typu konta użytkowników, komputery, drukarki, definiowanie uprawnień użytkowników do zasobów serwerowych oraz za pomocą obiektów zasad użytkowników i komputerów pracujących pod kontrolą systemów MS Windows następujących parametrów środowiska na komputerach lokalnych: - podłączanie lub usuwanie dysków sieciowych, - tworzenie, modyfikowanie lub usuwanie zmiennych środowiskowych, - tworzenie, modyfikowanie lub anulowanie udostępniania udziałów dyskowych, - tworzenie, modyfikowanie lub usuwanie połączeń drukarek lokalnych oraz dostępnych w sieci lokalnej za pomocą protokołu TCP/IP, - włączanie lub wyłączanie urządzeń sprzętowych lub klas urządzeń np. pamięci USB, - modyfikację menu głównego graficznego interfejsu użytkownika, - tworzenie, modyfikowanie lub usuwanie grup i użytkowników lokalnych, - tworzenie i modyfikację restrykcji dotyczących haseł (długość, okres ważności, złożoność) kont użytkowników lokalnych i sieciowych, - modyfikację ustawień lokalnej zapory sieciowej z możliwością ograniczania uprawnień administratora lokalnego.
5.	Możliwość wybrania w czasie instalacji polskiej lub angielskiej wersji językowej
6.	Program instalacyjny musi umożliwiać instalację oprogramowania zarówno na serwerach fizycznych i środowiskach wirtualnych.
7.	Licencja bezterminowa pozwalająca na instalację nielimitowanej ilości systemu serwerowego na 3 serwerach fizycznych:

	dwa serwery wyposażone w jeden procesor 16-rdzeniowy jeden serwer posiadający dwa procesory 12-rdzeniowe,
8.	Wymagana możliwość integracji z istniejącą usługą ActiveDirectory Zamawiającego opartego o MS Windows 2022 oraz migracji oprogramowania kontrolera do najnowszej wersji ActiveDirectory
9.	Należy dostarczyć najnowszą wersję oprogramowania udostępnianego przez producenta. Licencja musi umożliwiać instalację starszej wersji systemu (Downgrade) oraz przeniesienie na inną maszynę fizyczną.

Zamawiający nie dopuszcza licencji z rynku wtórego.

12. Wdrożenie.

Wykonawca dostarczy, zainstaluje i skonfiguruje dostarczone komponenty zgodnie z wytycznymi Zamawiającego.

Zakres wymaganych prac minimalnych:

Instalacja i konfiguracja dostarczonych urządzeń i oprogramowania a w szczególności:

Lp.	Zakres czynności
1.	Przygotowanie platformy sprzętowej serwera do backupu (konfiguracja BMC, aktualizacja firmware, konfiguracja RAID)
2.	Przygotowanie NAS (aktualizacja + konfiguracja)
3.	Przygotowanie biblioteki taśmowej (aktualizacja + konfiguracja)
4.	Instalacja oraz konfiguracja systemu operacyjnego na serwerze backupu
5.	Instalacja oraz konfiguracja oprogramowania do zabezpieczania danych na serwerze backupu
6.	Przygotowanie macierzy dyskowej (aktualizacja + konfiguracja)
7.	Przygotowanie nowych przełączników sieciowych
8.	Przygotowanie UPS (aktualizacja + konfiguracja)
9.	Przygotowanie UTM'a (aktualizacja + konfiguracja)
10.	Integracja nowego sprzętu z istniejącą infrastrukturą sieciową
11.	Utworzenie klastra wizualizacyjnego oraz migracja maszyn na macierz
12.	Konfiguracja oraz testowanie zadań kopii bezpieczeństwa
13.	Testowanie oraz weryfikacja środowiska + optymalizacja
14.	Dokumentacja
15.	Wsparcie powdrożeniowe w wymiarze 24h

VI Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

CPV 48820000-2 - serwery
CPV 48000000-8 – pakiety oprogramowania i systemy informatyczne
CPV 72263000-6 – usługi wdrażania oprogramowania
CPV 72268000-1 – usługi dostawy oprogramowania

VII Miejsce i Terminy wykonania zamówienia

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Dostawy sprzętu oraz oprogramowania będą realizowane w ciągu 60 dni, wdrożenia w ciągu 120 dni, liczonego od dnia podpisania umowy w przedmiocie udzielenia zamówienia publicznego.
Przedmiot umowy będzie dostarczany przez Wykonawcę do miejsc wskazanych przez Zamawiającego w zakresie dostawy sprzętu/oprogramowania/licencji.
Zamawiający może zawrzeć umowę w sprawie przedmiotowego zamówienia publicznego przed upływem terminu, jeżeli w przedmiotowym postępowaniu zostanie złożona tylko jedna oferta.

VIII Warunki udziału w postępowaniu

1. O udzielenie zamówienia mogą się ubiegać wykonawcy, którzy:
   - nie podlegają wykluczeniu na podstawie ustawy prawo zamówień publicznych,
   - spełniają warunki udziału w postępowaniu w zakresie kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile obowiązek ich posiadania wynika z odrębnych przepisów. Zamawiający nie określa szczegółowo ww. warunku.
   - spełniają warunki udziału w postępowaniu w zakresie sytuacji ekonomicznej lub finansowej. Zamawiający nie określa szczegółowo ww. warunku.
   - spełniają warunki udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej.
2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się odpowiednim doświadczeniem, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres wykonywania działalności jest krótszy, to w tym okresie zrealizował należycie co najmniej dwie dostawy sprzętu komputerowego na kwotę co najmniej 500 000 złotych brutto każda.
4. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
5. Wykonawca, który polega na zdolnościach innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

IX Przesłanki wykluczenia Wykonawcy

1. Zamawiający wykluczy wykonawcę z postępowania o udzielenie zamówienia, w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w art. 108 ust. 1 ustawy Pzp, tj.:

   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 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) 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 2021 r. poz. 523, 1292, 1559 i 2054),

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. poz. 769),
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;

2. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
3. 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.
4. 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.
5. Zamawiający nie wprowadza w tym postępowaniu dodatkowych podstaw wykluczenia wskazanych w art. 109 ustawy Pzp.
6. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp.
7. Jeżeli wykonawca polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby zamawiający zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.
8. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia zgodnie z art. 110 ust. 1 ustawy Pzp.
9. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt. 1, 2 i 5 ustawy Pzp, jeśli udowodni zamawiającemu, że spełnił przesłanki wskazane w art. 110 ust. 2 ustawy Pzp. Zamawiający oceni, czy podjęte przez wykonawcę czynności o których mowa w art. 110 ust. 2 ustawy Pzp są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w art. 110 ust. 2 ustawy Pzp, nie są wystarczające do wykazania rzetelności, zamawiający wykluczy wykonawcę.

10. Ponadto Zamawiający wykluczy z postępowania o udzielenie zamówienia Wykonawcę, w stosunku, do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 7 ust. 1 zgodnie z ustawą o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z dnia 13 kwietnia 2022 roku (Dz. U. z 2022, poz. 835).

X Obowiązek zatrudniania przez wykonawcę osób na podstawie stosunku pracy (art. 95 PZP)

1. Zamawiający wymaga aby osoby odpowiedzialne za koordynację wykonania zamówienia po Stronie Wykonawcy (pracownik administracyjny/biurowy/stanowisko równoważne) zatrudnione były na podstawie stosunku pracy, o którym mowa w art. 22 § 1 Kodeksu pracy.
2. Obowiązek określony powyżej dotyczy również podwykonawców.
3. W celu weryfikacji zatrudniania, przez wykonawcę lub podwykonawcę, na podstawie umowy o pracę, osób wykonujących wskazane przez zamawiającego czynności w zakresie realizacji zamówienia, Zamawiający wymaga złożenia oświadczenia wykonawcy lub podwykonawcy o zatrudnieniu pracownika na podstawie umowy o pracę.
4. Pozostałe osoby uczestniczące w wykonaniu zamówienia mogą współpracować z Wykonawcą na podstawie umów cywilnoprawnych.
5. W przypadku uzasadnionych wątpliwości co do przestrzegania prawa pracy przez Wykonawcę lub Podwykonawcę, Zamawiający może zwrócić się o przeprowadzenie kontroli przez Państwową Inspekcję Pracy.

XI Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania

1. Do oferty Wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu - zgodnie z **załącznikiem nr 3 do SWZ. Oświadczenie, o którym mowa w zdaniu pierwszym należy złożyć wraz ofertą.** W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie to składa każdy z Wykonawców. W przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, Wykonawca przedstawia, wraz z oświadczeniem własnym, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu lub kryteriów selekcji, w zakresie, w jakim wykonawca powołuje się na jego zasoby. Oświadczenia to składa się pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej, opatrzonej podpisem zaufanym lub podpisem osobistym. Informacje zawarte w ww. oświadczeniu stanowią wstępne potwierdzenie, że Wykonawca spełnia warunki udziału w postępowaniu oraz nie podlega wykluczeniu z postępowania.
2. Zgodnie z art. 274 ust. 1 ustawy Pzp, zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych:

- oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:
  a) art. 108 ust. 1 pkt 3 ustawy,
  b) art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
  c) art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
  d) art. 108 ust. 1 pkt 6 ustawy

według wzoru stanowiącego Załącznik nr 4 do SWZ;

- wykazu dostaw wykonanych w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane oraz załączeniem dowodów określających, czy te dostawy zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy; według wzoru stanowiącego Załącznik nr 5 do SWZ;
- 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 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej; według wzoru stanowiącego Załącznik nr 6 do SWZ.

3. W odniesieniu do pozostałych przedmiotowych środków dowodowych zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy spełniają określone przez zamawiającego wymagania, cechy i kryteria.
4. Zamawiający informuje, że działając na podstawie art. 107 ust. 2 ustawy Pzp przewiduje, że w sytuacji, w której Wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający jednokrotnie wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.

XII Poleganie na zasobach podmiotów trzecich

1. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby składa wraz z ofertą zobowiązanie podmiotu trzeciego do oddania 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.
2. Zobowiązanie podmiotu udostępniającego zasoby potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   - zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
   - sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   - czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy lub usługi, których wskazane zdolności dotyczą.
3. Podwykonawcy obowiązani są do złożenia wszelkich oświadczeń, w szczególności oświadczeń sankcyjnych i o braku przesłanek wykluczenia w takim zakresie w jakim dotyczą one Wykonawcy.

XIII Podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
2. Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

XIV Informacja dla wykonawców polegających na zasobach innych podmiotów, na zasadach określonych w art. 118 ustawy PZP

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
4. 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.
5. Zobowiązanie podmiotu udostępniającego zasoby lub inny środek dowodowy, o którym mowa w pkt 9.4 SWZ 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;
   3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
6. Zamawiający oceni, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu a także zbada, czy nie zachodzą, wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
7. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą, wobec tego podmiotu podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
8. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia 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.

XV Kryterium równoważności

Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym przez Zamawiającego. Wykonawca oferując rozwiązanie równoważne do opisanego powyżej jest zobowiązany wykazać (udowodnić) równoważność w zakresie wskazanych parametrów, które muszą być na poziomie nie gorszym niż parametry wskazane przez Zamawiającego - Wykonawca musi wykazać (udowodnić), iż proponowane rozwiązanie w równoważnym stopniu spełnia wymagania określone w zapytaniu ofertowym, w szczególności w zakresie parametrów. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do określonego wyrobu, źródła, znaków towarowych, patentów czy pochodzenia lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć,

że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych, w szczególności o parametrach technicznych, użytkowych, funkcjonalnych i jakościowych nie gorszych niż te, podane w opisie przedmiotu zamówienia.

XVI Opis sposobu składania ofert w postępowaniu

1. Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej.
2. Postępowanie prowadzone jest w języku polskim za pośrednictwem Platformy zakupowej pod adresem profilu nabywcy: https://platformazakupowa.pl/pn/dobrzyniewo, w zakładce dedykowanej postępowaniu (pod nazwą postępowania wskazaną w tytule SWZ).
3. **Wykonawca może złożyć ofertę za pośrednictwem Platformy. Złożenie więcej niż jednej oferty w ramach niniejszego zamówienia spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę. Platforma szyfruje Oferty w taki sposób, że nie jest możliwe zapoznanie się z ich treścią, do terminu wyznaczonego na otwarcie ofert.**
4. Na ofertę, składają się:
   a) formularz ofertowy - (Załącznik nr 1 do SWZ),
   b) oświadczenie o niepodleganiu wykluczeniu i spełnianiu warunków udziału (Załącznik nr 3 do SWZ),
   c) pełnomocnictwo – w przypadku, gdy oferta została podpisana przez pełnomocnika lub gdy ofertę składają Wykonawcy wspólnie ubiegający się o udzielenie zamówienia zgodnie z art. 58 ustawy PZP. Pełnomocnictwo powinno być udzielone przez osoby uprawnione do reprezentowania Wykonawcy.
   d) Dokumenty, z których wynika prawo do podpisania oferty (oryginał w postaci dokumentu elektronicznego, opatrzony elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym; Zamawiający dopuszcza złożenie elektronicznej kopii pełnomocnictwa poświadczonej przez notariusza kwalifikowalnym podpisem elektronicznym) względnie do podpisania innych dokumentów składanych z ofertą, chyba że Zamawiający może je uzyskać w szczególności za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności w rozumieniu ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności realizujących zadania publiczne.
5. Treść oferty musi odpowiadać warunkom zamówienia.
6. Ofertę wraz z załącznikami sporządza się pod rygorem nieważności w formie elektronicznej i opatruje elektronicznym kwalifikowanym podpisem lub w postaci elektronicznej i opatruje podpisem zaufanym lub podpisem osobistym.
7. Oferty należy sporządzić w języku polskim na **formularzu ofertowym** zgodnie z **Załącznikiem nr 1 do SWZ**.
8. Oferta wraz z załącznikami musi być sporządzona w sposób czytelny.
9. Oferta wraz z załącznikami winna być podpisana przez osobę/y upoważnioną/e do reprezentowania Wykonawcy i składania oświadczeń woli w imieniu Wykonawcy, wskazaną/e we właściwym rejestrze lub posiadającą/e odpowiednie umocowanie (dokument potwierdzający umocowanie.
10. Oferta powinna być sporządzona w języku polskim, z zachowaniem formy elektronicznej pod rygorem nieważności, w postaci elektronicznej w formacie danych: .rtf; .pdf; .xps; .odt; .ods; .doc; .docx i podpisana elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca sporządzenie dokumentu elektronicznego w postaci .pdf.
11. Podpisy kwalifikowane wykorzystywane przez Wykonawców do podpisywania wszelkich plików muszą spełniać "Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".
12. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików XAdES.
13. Oferta nie może być złożona za pomocą poczty elektronicznej Zamawiającego.

14. Złożenie oferty wraz z załącznikami na nośniku danych (np. CD, pendrive) nie stanowi jego złożenia przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy o świadczeniu usług drogą elektroniczną.
15. Dokumenty, oświadczenia (formularze, załączniki) wchodzące w skład oferty muszą być podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym przez właściwe osoby ze względu na rodzaj dokumentu (odpowiednio Wykonawca, członek konsorcjum, podmiot na którego zasoby Wykonawca się powołuje, reprezentant banku lub ubezpieczyciel, notariusz, itp.). Oświadczenia, w tym sporządzane na podstawie wzorów stanowiących formularze do SWZ powinny być złożone w oryginale w postaci dokumentu elektronicznego.
16. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.
17. Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert.
18. Wymagania techniczne i organizacyjne związane z wykorzystaniem Platformy zakupowej:
    a) w postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawca odbywa się przy użyciu Platformy (adres: https://platformazakupowa.pl/pn/dobrzyniewo) przez dostępny na stronie danego postępowania formularz **„Wyślij wiadomość”;**
    b) wymagania techniczne i organizacyjne wysyłania oraz odbierania dokumentów elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu zostały opisane w Regulaminie korzystania z Platformy (adres: https://platformazakupowa.pl/pn/dobrzyniewo). Składając ofertę Wykonawca akceptuje Regulamin Internetowej Platformy zakupowej platformazakupowa.pl firmy Open Nexus Sp. z o.o. dla Użytkowników (Wykonawców);
    c) Zamawiający informuje, że posiadanie konta na Platformie jest dobrowolne, a złożenie oferty w przetargu jest możliwe bez posiadania konta. Wykonawca nieposiadający konta na Platformie Zakupowej może za jej pośrednictwem wprowadzić zmiany do złożonej ofert. Wykonawca niezalogowany nie może samodzielnie wycofać oferty. W celu wycofania oferty należy skontaktować się z Centrum Wsparcia Klienta, które służy pomocą techniczną od godziny 7:00 do godziny 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mail: cwk@platformazakupowa.pl. Na Platformie Zakupowej w zakładce „Instrukcje dla wykonawców” opisana jest szczegółowa procedura zmiany i wycofania oferty. Po upływie terminu składania ofert Wykonawca skutecznie dokonać zmiany ani wycofać złożonej oferty;
    d) na stronie Platformy zakupowej znajduje się Instrukcja dla Wykonawców;
    e) W przypadku pytań dotyczących funkcjonowania i obsługi technicznej Platformy zakupowej, prosimy o skorzystanie z pomocy Centrum Wsparcia Klienta, które udzieli wszelkich informacji związanych z procesem składania ofert, rejestracji czy innych aspektów technicznych platformy. Centrum Wsparcia Klienta dostępne jest codziennie od poniedziałku do piątku w godzinach od 7:00 do 17:00 pod numerem tel. 22 101 02 02 lub za pośrednictwem adresu e-mail: cwk@platformazakupowa.pl.
19. Zamawiający, zgodnie z art. 223 ust. 2 ustawy PZP, poprawia w ofercie:
    a) oczywiste omyłki pisarskie,
    b) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
    c) inne omyłki polegające na niezgodności oferty z SWZ, niepowodujące istotnych zmian w treści oferty
    – niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
20. Wykonawca ponosi wszelkie koszty związane z przygotowaniem oferty.
21. Oferta wraz z wymaganymi załącznikami, oświadczeniami i dokumentami jest jawna, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji, a Wykonawca nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnice przedsiębiorstwa. Wykonawca nie może zastrzec informacji podawanych do publicznej wiadomości podczas otwarcia ofert (art. 222 ust. 5 ustawy PZP). Wszelkie informacje

stanowiące tajemnice przedsiębiorstwa powinny zostać złożone w osobnym polu składania oferty przeznaczonym na zamieszczenie tajemnicy przedsiębiorstwa.

22. Zgodnie z art. 18 ust. 3 ustawy PZP, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli Wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
23. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
24. Jeżeli oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia została wybrana, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców.
25. Ofertę wraz z oświadczeniami i dokumentami należy złożyć w terminie **do dnia 30.04.2025 r. do godz. 10:00** za pośrednictwem platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/dobrzyniewo.
26. Otwarcie ofert nastąpi w dniu **30.04.2025 r. po godz. 10:30.**
27. Wykonawca może przed upływem terminu składania ofert wycofać ofertę.

XVII Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia) (C)	60
2.	Procesor serwera do wykonywania kopii zapasowych (E)	20
3.	Gwarancje dla urządzeń – (serwer kopi zapasowych, macierz dyskowa, serwer do wykonywania kopii zapasowych z narzędziami do wirtualizacji, serwer NAS) (F)	20

2. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.
3. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
4. Przy ocenie ofert w kryterium „Cena” (C) punkty zostaną przyznane w poniższy sposób:
   - Cena – znaczenie 60% (maksymalnie do 60 pkt)
   - Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
   - Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

C = CC min/ CC of x 60

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena”

CC min – najniższa cena brutto spośród badanych ofert

CC of – cena brutto badanej ofert

- Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 1 do SWZ.

5. Kryterium „Procesor serwera do wykonywania kopii zapasowych" stanowi 20 możliwych do uzyskania punktów:
   - Do 16 rdzeni włącznie – 20 pkt
   - Powyżej 16 rdzeni do 24 włącznie – 10 pkt
   - Powyżej 24 rdzeni – 0 pkt
   Zamawiający wyjaśnia, że premiuje liczbę rdzeni, która jest dla niego jak najbardziej optymalna, z uwagi na
6. Kryterium „Gwarancje dla urządzeń – (serwer kopii zapasowych, macierz dyskowa, serwer do wykonywania kopii zapasowych z narzędziami do wirtualizacji, serwer NAS)" stanowi 20 możliwych do uzyskania punktów:
   - Wydłużenie gwarancji do 60 miesięcy – 20pkt
   - Wydłużenie gwarancji do 48 miesięcy – 10pkt
   - 36 miesięcy – 0pkt
7. Sumaryczna liczba punktów zostanie obliczona według wzoru:
   W = C + E + F

   gdzie:

   W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

   C – liczba punktów przyznanych w kryterium „Cena",

   E – wartość punktowa kryterium „Procesor serwera do wykonywania kopii zapasowych",

   F – wartość punktowa kryterium „Gwarancje dla urządzeń – (serwer kopi zapasowych, macierz dyskowa, serwer do wykonywania kopii zapasowych z narzędziami do wirtualizacji, serwer NAS)"

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku
8. Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

XVIII Wzór umowy

Wzór Umowy stanowi Załącznik nr 2 do SWZ.

XIX 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 danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO") informujemy, że:

1) administratorem Pani/Pana danych osobowych jest Gmina Dobrzyniewo Duże z siedzibą w Dobrzyniewie Dużym przy ulicy Białostockiej 25 reprezentowana przez Wójta.
2) administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: iod@eterneco.eu
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie przetargu nieograniczonego.

4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 ustawy PZP
5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 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 bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy PZP, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
8) posiada Pani/Pan:
   a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia);
   b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (*skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą PZP oraz nie może naruszać integralności protokołu oraz jego załączników*);
   c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (*prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*);
   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 RODO;
10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

XX 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. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/dobrzyniewo
2. Komunikacja między Zamawiającym, a Wykonawcą odbywa się przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną za pośrednictwem **formularza „Wyślij wiadomość”** dostępnego na stronie internetowej profilu nabywcy: https://platformazakupowa.pl/pn/dobrzyniewo w zakładce dedykowanej postępowaniu. Formularz **„Wyślij wiadomość”** służy do zadawania pytań Zamawiającemu oraz przesyłania dokumentów, o których uzupełnienie wezwał Wykonawcę Zamawiający. **UWAGA:** formularz **„Wyślij wiadomość”** służy wyłącznie do

komunikacji, a nie do składania ofert. Składanie ofert musi odbywać się poprzez formularz ofertowy dostępny na stronie postępowania, zgodnie z instrukcją zawartą w linku na stronie postępowania. Ofertę Wykonawca może złożyć wyłącznie za pośrednictwem Platformy zakupowe.

3. W sytuacjach awaryjnych np. w przypadku przerwy w funkcjonowaniu lub awarii lub niedziałania https://platformazakupowa.pl/pn/dobrzyniewo Zamawiający może również komunikować się z Wykonawcami za pomocą poczty elektronicznej, na adres: m.bielaga@dobrzyniewo.pl, z zastrzeżeniem, że Ofertę Wykonawca może złożyć wyłącznie za pośrednictwem Platformy Zakupowej.
4. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę razem z ofertą za pośrednictwem formularza ofertowego dostępnego na Platformie na stronie postępowania.
5. Zgodnie z treścią art. 63 ust. 2 ustawy PZP Ofertę oraz oświadczenia sporządza się pod rygorem nieważności w formie elektronicznej i opatruje elektronicznym kwalifikowanym podpisem lub w postaci elektronicznej i opatruje podpisem zaufanym lub podpisem osobistym.
6. Za datę przekazania oświadczeń, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich doręczenia za pośrednictwem formularza zamieszczonego na stronie internetowej profilu nabywcy https://platformazakupowa.pl/pn/dobrzyniewo dostępnego w zakładce dedykowanej postępowaniu.
7. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
8. Zamawiający, zgodnie z § 11 ust. 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 dzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r. poz. 2452; określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.:
   1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   2) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
   3) zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
   4) włączona obsługa JavaScript,
   5) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   6) Platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
   7) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
9. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   1) akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
   2) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem.
10. **Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl**, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego"). Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 Ustawy Prawo Zamówień Publicznych.
11. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności

podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

12. Udzielenie wyjaśnień do treści Specyfikacji Warunków Zamówienia
    1) Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji Warunków Zamówienia. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przez upływem terminu składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
    2) Jeżeli wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął po upływie terminu składania wniosku, o którym mowa w pkt 1), lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpatrywania.
    3) Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w pkt.1).
    4) Treść zapytań wraz z wyjaśnieniami Zamawiające przekaże Wykonawcom, którym przekazał SWZ, bez ujawnienia źródła zapytania oraz na stronie internetowej profilu nabywcy, na której zamieszczona jest SWZ - https://platformazakupowa.pl/pn/dobrzyniewo.
    5) W przypadku rozbieżności pomiędzy treścią niniejszej SWZ, a treścią udzielonych wyjaśnień lub zmian SWZ, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
    6) Zamawiający nie będzie udzielał ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane do Zamawiającego zapytania, w sprawach wymagających zachowania formy pisemnej. Uzyskane odpowiedzi nie będą wiążące dla Zamawiającego i Wykonawców.
    7) W uzasadnionych przypadkach Zamawiający może przez upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę SWZ Zamawiający udostępni na stronie internetowej profilu nabywcy https://platformazakupowa.pl/pn/dobrzyniewo, na której udostępniona jest SWZ.
    8) Jeżeli w wyniku zmiany treści SWZ nieprowadzącej do zmiany treści ogłoszenia o zamówieniu będzie niezbędny dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania ofert i poinformuje o tym wykonawców, którym przekazano SWZ oraz zamieści informacje na stronie internetowej profilu nabywcy https://platformazakupowa.pl/pn/dobrzyniewo, na której udostępniona jest SWZ.
    9) Jeżeli zmiana treści SWZ, będzie prowadziła do zmiany treści ogłoszenia o zamówieniu, Zamawiający dokona zmiany treści ogłoszenia o zamówieniu w sposób przewidziany w art. 271 ustawy PZP (tj. zamieści ogłoszenie o zmianie ogłoszenia w Biuletynie Zamówień Publicznych).
    10) Zamawiający nie zamierza zwoływać zebrania Wykonawców przed składaniem ofert.
13. Rozszerzenia plików wykorzystywanych przez Wykonawców powinny być zgodne z Załącznikiem nr 2 do "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", zwanego dalej Rozporządzeniem KRI.
14. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .docx .xls .xlsx .jpg (.jpeg) ze szczególnym wskazaniem na .pdf
15. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z rozszerzeń:
    a) .zip
    b) .7Z
16. Wśród rozszerzeń powszechnych a **niewystępujących** w Rozporządzeniu KRI występują: .rar .gif .bmp .numbers .pages. **Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.**
17. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi **maksymalnie 10MB**, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi **maksymalnie 5MB**.
18. W przypadku stosowania przez wykonawcę kwalifikowanego podpisu elektronicznego:

- Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu zamawiający zaleca, w miarę możliwości, **przekonwertowanie plików składających się na ofertę na rozszerzenie .pdf i opatrzenie ich podpisem kwalifikowanym w formacie PAdES.**
- Pliki w innych formatach niż PDF **zaleca się opatrzyć podpisem w formacie XAdES o typie zewnętrznym**. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
- Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.

19. Zamawiający zaleca aby **w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju.** Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
20. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
21. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
22. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
23. Jeśli Wykonawca pakuje dokumenty np. w plik o rozszerzeniu .zip, zaleca się wcześniejsze podpisanie każdego ze skompresowanych plików.
24. Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty.

XXI Sposób obliczenia ceny

1. Wykonawca poda cenę oferty w Formularzu Ofertowym jako cenę brutto [z uwzględnieniem kwoty podatku od towarów i usług (VAT)] z wyszczególnieniem stawki podatku od towarów i usług (VAT).
2. Cena oferty stanowi wynagrodzenie ryczałtowe.
3. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca poda w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty,
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

XXII Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający zawiera umową w sprawie zamówienia publicznego, z uwzględnieniem art. 577 pzp, 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 umową w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertą.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.

4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią Załącznik Nr 2 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą 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 albo unieważnić postępowanie.

XXIII Środki ochrony prawnej

1. Środki ochrony prawnej przewidziane są w dziale IX ustawy.
2. Środkami ochrony prawnej są odwołanie i skarga do sądu.
3. Środki ochrony prawnej przysługują wykonawcy 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. 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 ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
4. Odwołanie przysługuje na:
   1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy;
   3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.
5. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Terminy wnoszenia odwołań.
   1) Odwołanie wnosi się w terminie:
   a) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
   b) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a.
7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.
8. Odwołanie w przypadkach innych niż określone w pkt 1 i 2 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne.
9. Jeżeli zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy lub mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty lub nie zaprosił wykonawcy do złożenia oferty w ramach dynamicznego systemu zakupów lub umowy

ramowej, odwołanie wnosi się nie później niż w terminie:

1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania
2) miesiąca od dnia zawarcia umowy, jeżeli zamawiający:
   a) nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo
   b) zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o wyniku postępowania, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki.

10. Odwołanie zawiera:

1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);
2) nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;
3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;
4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku – numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;
5) określenie przedmiotu zamówienia;
6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych albo publikacji w Dzienniku Urzędowym Unii Europejskiej;
7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, lub wskazanie zaniechania przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy;
8) zwięzłe przedstawienie zarzutów;
9) żądanie co do sposobu rozstrzygnięcia odwołania;
10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności; podpis odwołującego albo jego przedstawiciela lub przedstawicieli;
11) wykaz załączników.

11. Do odwołania dołącza się:
    1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;
    2) dowód przekazania odpowiednio odwołania albo jego kopii zamawiającemu;
    3) dokument potwierdzający umocowanie do reprezentowania odwołującego.
12. Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych.

ZAŁĄCZNIKI

Załącznik nr 1 Formularz oferty,
Załącznik nr 2 Istotne Postanowienia Umowy,
Załącznik nr 3 Oświadczenie wykonawcy z art. 125 Pzp,
Załącznik nr 4 Wzór oświadczenia o aktualności informacji,
Załącznik nr 5 Wzór wykazu dostaw,
Załącznik nr 6 Wzór oświadczenia o grupie kapitałowej.