Obsza, 16.02.2026 r.

OŚ.2710.4.2026

ZAPYTANIE O USTALENIE WARTOŚCI ZAMÓWIENIA

Niniejsze zapytanie nie stanowi zaproszenia do składania ofert w rozumieniu przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2024 r. poz. 1061 ze zm.) i podstawy do udzielenia zamówienia w rozumieniu przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2024 r. poz. 1320 ze zm.).

Zgodnie z Rozdziałem 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2024 r. poz. 1320 ze zm.) Zamawiający przed wszczęciem postępowania zobowiązany jest do ustalenia wartości zamówienia.

W celu ustalenia wartości zamówienia, Zamawiający zaprasza potencjalnych Wykonawców do zapoznania się z załączoną informacją o wymaganiach dotyczących przedmiotu zamówienia i złożenia informacji dotyczącej szacunkowej wartości zamówienia.

Gmina Obsza z siedzibą w Obszy, Obsza 36, 23-413 Obsza w ramach realizacji projektu pn. **„Podniesienie poziomu cyberbezpieczeństwa w Gminie Obsza”** realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, w ramach Projektu grantowego „Cyberbezpieczny samorząd” zwraca się z prośbą o wstępne oszacowanie wartości zamówienia, zgodnie z poniższym opisem

I. PRZEDMIOT ZAMÓWIENIA:

Podniesienie poziomu cyberbezpieczeństwa w Gminie Obsza w ramach projektu „Cyberbezpieczny Samorząd” FERC.02.02-CS.01-001/23/1402 z dnia 13-12-2023

II. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA:

Przedmiotem zamówienia jest dostawa i uruchomienie sprzętu informatycznego na potrzeby tworzenia i weryfikacji kopii bezpieczeństwa zgodnie z poniższym zestawieniem:

1. Serwer z oprogramowaniem – 2 szt.
2. Macierz dyskowa – 1 szt.
3. Bibliotek taśmowa – 1 szt.
4. Oprogramowanie do backupu – 1 szt.
5. Przełącznik dostępowy – 2 szt.

III. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Serwer z oprogramowaniem – 2 sztuki, 3 lata gwarancji NBD, uszkodzone dyski twarde pozostają u Zamawiającego, licencja wieczysta na system operacyjny
Wymagane minimalne parametry techniczne

1. **Obudowa**
   - Obudowa Rack o wysokości max 1U
   - Obudowa dyskowa nie jest wymagana. Zamawiający nie przewiduje montażu dysków.
   - Obudowa wyposażona w ozdobną ramkę chroniącą dyski przed nieuprawniony dostępem.
2. **Płyta główna**
   - Płyta główna z możliwością zainstalowania do dwóch procesorów.

- Obsługa procesorów 144 rdzeniowych.
- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
- Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci
- Płyta główna powinna obsługiwać do 4TB pamięci RAM.

3. **Chipset**
   - Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
4. **Procesor**
   - Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.3GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 199 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera.
5. **RAM**
   - 256GB DDR5 RDIMM 6400MT/s, w modułach po 32GB
6. **Kontroler RAID**
   - Nie jest wymagany
7. **Dyski twarde** Zainstalowane:
   - Zainstalowany 1 dysk M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
8. **Gniazda PCI**
   - Dwa sloty PCIe FH x16 gen.5
9. **Interfejsy sieciowe/FC/SAS**
   - 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
   - 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 – karta PCIe wraz z wkładkami 10Gb SFP+
   - 2 interfejsy 32GB FC wraz z wkładkami – karta PCIe
10. **Wbudowane porty**
    - 4 porty USB w tym min:
      a. 1 port USB 2.0 Type-C
      b. 2 porty USB 3.1
      c. 1 port USB 3.1 wewnątrz obudowy
    - Port VGA z tyłu obudowy
11. **Video**
    - Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
12. **Zasilacze**
    - Redundantne, Hot-Plug min. 800W klasy Titanium
    - 2x przewód C13/C14 o dł. min. 2 metry
13. **Elementy montażowe**
    - Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
    - Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych – nie jest wymagane.
14. **System operacyjny/dodatkowe oprogramowanie**
    - Windows Server 2025 Standard – licencja dobrana tak, aby umożliwić uruchomienie 2 maszyn wirtualnych
15. **Bezpieczeństwo**

- Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
- Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0
- Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

16. Karta Zarządzania

Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
- szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika,
- możliwość podmontowania zdalnych wirtualnych napędów,
- wirtualną konsolę z dostępem do myszy, klawiatury,
- wsparcie dla IPv6,
- wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer,
- integracja z Active Directory,
- możliwość obsługi przez sześciu administratorów jednocześnie,
- Wsparcie dla automatycznej rejestracji DNS,
- wsparcie dla LLDP,
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej,
- możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy,
- Monitorowanie zużycia dysków SSD,
- Automatyczne zgłaszanie alertów do centrum serwisowego producenta,
- Automatyczne update firmware dla wszystkich komponentów serwera,
- Możliwość przywrócenia poprzednich wersji firmware,
- Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON,
- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych,
- Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.

17. Oprogramowanie do zarządzania

- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.
- integracja z Active Directory.
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta.
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.
- Szczegółowy opis wykrytych systemów oraz ich komponentów.
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF.
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika.
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.
- Szybki podgląd stanu środowiska.
- Podsumowanie stanu dla każdego urządzenia.
- Szczegółowy status urządzenia/elementu/komponentu.
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.
- Integracja z service desk producenta dostarczonej platformy sprzętowej.
- Możliwość przejęcia zdalnego pulpitu.
- Możliwość podmontowania wirtualnego napędu.
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów.
- Możliwość importu plików MIB.
- Przesyłanie alertów „as-is” do innych konsol firm trzecich.
- Możliwość definiowania ról administratorów.
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania).
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta.
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

18. Oprogramowanie do monitorowania

Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

- Monitoring:
  - ilość podłączonych oraz rozłączonych systemów,
  - stan podłączonych urządzeń,
  - informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów,
  - Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia,
  - informacje o statusie gwarancji dla poszczególnych urządzeń,
  - informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń,
  - informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych,
  - wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych,
  - wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych,
  - monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych,
  - zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC,
  - szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej,
  - monitoring parametrów serwerów z informacją o minimum:
    - Obciążeniu procesora
    - Zużyciu pamięci RAM
    - Temperaturze procesorów
    - Temperaturze powietrza wlotowego
    - Zużyciu prądu
    - Zmianach w fizycznej konfiguracji serwera
    - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach,
  - monitoring parametrów pamięci masowych z informacją o minimum:
    - Opóźnieniach
    - IOPS
    - Przepustowości
    - Utylizacji kontrolerów
    - Pojemność całkowita i dostępna
    - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
    - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
    - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
    - Informacje o poziomie redukcji danych

        - Informacje o statusie replikacji oraz snapshotów
    - monitoring parametrów przełączników sieciowych z informacją o minimum:
        - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
        - Stanie komponentów: zasilacze, wentylatory
        - Podłączonych hostach
        - Ilości i statusu portów
        - Utylizacji procesora
        - Utylizacji poszczególnych portów
        - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach,
- Aktualizacja firmware
    - możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
    - możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
    - możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania
    - możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
    - możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
    - Możliwość generowania raportów dla serwerów zawierających informację o:
        - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej.
        - Średnim obciążeniu: procesorów, pamięci RAM, IO,
    - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
        - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji.
    - Generowanie raportów do plików CSV i PDF.
- Cyberbezpieczeństwo
    - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
    - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
    - Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
    - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
    - Urządzenie Producenta dostarczane w ramach postępowania
    - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent

- Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;

- Możliwość rozszerzenia funkcjonalności
  - Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
- Inne

  Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android.

19. Certyfikaty

- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001
- Serwer musi posiadać deklaracja CE.
- Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver,według normy wprowadzonej w 2019 r.

20. Dokumentacja użytkownika

- Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

21. Warunki gwarancji

- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.
- Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
- Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
- Uszkodzone dyski pozostają własnością zamawiającego.
- Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
  a. Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
  b. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
  c. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
  d. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.

e. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

22. Dodatkowa 1 sztuka karty SAS do podłączenia biblioteki taśmowej.

23. Przygotowanie i realizacja projektu technicznego i planu migracji użytkowanej poczty elektronicznej:

- przygotowanie 2 serwerów pocztowych
  - serwer poczty główny,
  - serwer poczty zapasowy pełniący funkcję archiwum,
  - uruchomienie replikacji poczty wchodzącej i wychodzącej,
  - uruchomienie filtrów antispam a serwerach poczty,
  - uruchomienie antivirusa na poziomie serwera poczty,
  - konfiguracja skrzynek pocztowych dla użytkowników (do 50 skrzynek),
  - konfiguracja backup, serwera poczty, skrzynki, maila.
- testy odzyskiwania serwera pocztowego, pojedynczej skrzynki jak i pojedynczego maila,
- migracja istniejących skrzynek pocztowych do nowego serwera poczty do 50 skrzynek,
- wsparcie przy przełączeniu poczty na nowy serwer poczty,
- warsztaty dla administratorów 1 dzień.

24. Migracja danych z istniejącego środowiska Zamawiającego na nowo wdrożone urządzenia i systemy:

- Active Directory,
- System dziedzinowy,
- elektroniczny obieg dokumentów,
- Serwer plikowy**.**

25. Weryfikacja poprawności działania połączeń:

- Testy funkcjonowania środowiska,
- integracji wszystkich komponentów i poprawności działania kopii zapasowych oraz usług katalogowych.

26. instalacja, konfiguracja oraz uruchomienie systemu SIEM (Security Information and Event Management) — licencja open source, w ilości 1 sztuka, wraz ze szkoleniem personelu

- Dostawa nośników instalacyjnych i licencji open source SIEM.
- Instalacja i konfiguracja systemu SIEM.
- Integracja z istniejącą infrastrukturą sieciową i systemową.
- Migracja i konfiguracja agentów na systemach Windows, Linux i urządzeniach sieciowych.
- Implementacja polityk detekcji, korelacji i reakcji.
- Opracowanie i wdrożenie procedur backupu oraz Disaster Recovery.
- Szkolenie administracyjne i techniczne personelu

System zapewnia zbieranie zdarzeń i logów z różnorodnych źródeł: serwery, urządzenia sieciowe (firewalle, przełączniki), systemy IDS/IPS, aplikacje, bazy danych.
System obsługuje protokoły: Syslog, SNMP, WMI, REST API, JSON oraz inne standardowe kanały transmisji logów, a także normalizację i kategoryzację logów do jednolitego formatu analitycznego.
System pozwala na definiowanie reguł korelacji opartych na branżowych standardach (MITRE ATT\&CK, OWASP).
System posiada wbudowane i konfigurowalne mechanizmy detekcji anomalii na poziomie sieci (NIDS) i hosta (HIDS).

System zapewnia integrację informacji o podatnościach z bazą CVE i skanerów zewnętrznych.
System generuje i wysyła alerty do personelu odpowiedzialnego (e-mail, SMS, webhook).
System zapewnia automatyczne reakcje na wybrane zdarzenia (blokowanie IP, izolacja hosta).
System zapewnia integrację z systemami ticket-owymi (np. JIRA, ServiceNow).
System zapewnia generowanie raportów ad-hoc i okresowych (dziennych, tygodniowych, miesięcznych).
System zapewnia tworzenie niestandardowych dashboardów i widoków dla różnych grup odbiorców (Kierownictwo, Dział IT, Audyt).
System zapewnia eksport raportów w formatach PDF, HTML, CSV.System posiada intuicyjny, webowy interfejs administracyjny i analityczny oraz API do automatyzacji zadań i integracji z zewnętrznymi systemami.
System zapewnia uwierzytelnianie użytkowników (LDAP/AD, RADIUS) w oparciu o role i uprawnienia z granularną kontrolą dostępu oraz szyfrowanie komunikacji (TLS/HTTPS) oraz ochronę danych w spoczynku.

27. Montaż wszystkich urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego.
28. Podłączenie do sieci zasilania zgodnie z wytycznymi Zamawiającego.
29. Uruchomienie i weryfikacja poprawności działania urządzeń.
30. Aktualizacja oprogramowania do wersji zalecanej przez producenta.
31. Konfiguracja podstawowych usług sieciowych i zarządzających: adresacja IP, NTP, DNS.
32. Instalacja i konfiguracja maszyn wirtualnych (np. serwer Windows).
33. Tworzenie wzorcowego obrazu maszyny wirtualnej.
34. Konfiguracja usług klastra wirtualizacji, w tym definiowanie sieci wirtualnych.
35. Włączenie funkcji serwera usług katalogowych na maszynie wirtualnej.
36. Konfiguracja polityk usług katalogowych dotyczących urządzeń i użytkowników.
37. Konfiguracja profili użytkowników i dostępów do zasobów.
38. Dokumentacja powykonawcza dla całego środowiska Zamawiającego
- Topologia logiczna i fizyczna rozwiązania.
- Opis wdrożonych systemów i konfiguracji urządzeń.
- Poświadczenia dostępowe i zestawienie konfiguracji wszystkich komponentów.

2. Macierz dyskowa – 1 sztuka, 3 lata gwarancji NBD, uszkodzone dyski twarde pozostają u Zamawiającego
Wymagane minimalne parametry techniczne

1. Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.
2. Minimum dwa kontrolery pracujące w trybie Symmetrical Active-Active (SAN-only), to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery muszą pozwalać na udostępnianie zasobów protokołem FC, iSCSI w zależności od zastosowanych kart komunikacyjnych.
3. Komunikacja pomiędzy parą kontrolerów (synchronizacja cache) macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband.
4. Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze wielu kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego.

5. Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 2 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązanie oparte o wirtualizator.
6. Macierz musi umożliwiać rozbudowę do co najmniej 4 par kontrolerów dyskowych tworzących jedna logiczną macierz, bez konieczności wymiany zaoferowanej pary kontrolerów.
7. Macierz musi być skonstruowana wyłącznie do obsługi modułów pamięci SSD i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych.
8. Całkowita pojemność brutto (fizyczna) urządzenia musi wynosić minimum 38 TB i musi być zbudowana wyłącznie w oparciu o moduły pamięci SSD. Rozmiar pojedynczego modułu nie może być większy niż 4 TB.
9. Macierz musi umożliwiać rozbudowę do co najmniej 70 sztuk oferowanego typu modułów pamięci, bez wymiany kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek i modułów SSD)
10. Kontrolery łącznie muszą być wyposażone w procesory o sumarycznej ilości min. 48 rdzeni (ang.: core). Procesory w macierzy muszą obsługiwać protokół PCI Express Generacji 4.
11. Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.
12. Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
13. Macierz musi posiadać minimum 4 porty 10Gb/s obsługujące protokół iSCSI. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), wymaga się ich dostarczenia wraz z urządzeniem.
14. Możliwość rozbudowy macierzy o minimum 8 portów 25Gb/s obsługujących protokół w ramach zaoferowanej ilości kontrolerów oraz możliwość podłączania serwerów bezpośrednio do tych portów macierzy bez użycia przełączników. Możliwość rozbudowy o wskazane porty nie może ograniczać rozbudowy do wymaganej ilości modułów pamięci.
15. Urządzenie musi obsługiwać poziomy RAID5 i RAID6 (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare) lub równoważne poziomy RAID zabezpieczające przed awarią dwóch dysków jednocześnie.
16. Macierz musi umożliwiać skonfigurowanie poziomu RAID zapewniającego odporność na jednoczesną awarię 3 dysków w grupie RAID.
17. Brak pojedynczego punktu awarii. Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy.
18. Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap.
19. Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
20. Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie

wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów SSD. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI co najmniej 1 rok wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożlwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

21. Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 2000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
22. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
23. Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii).

24. Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
25. Macierz musi mieć możliwość włączenia funkcjonalności kompresji danych w trybie in-line, a ponadto musi ona umożliwiać:
    - włączenie kompresji dla poszczególnych wolumenów,
    - wyłączenie kompresji dla poszczególnych wolumenów na których wcześniej kompresja była włączona,

    Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
26. Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
27. Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać klastrownie wybranych woluminów bez konieczności

stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

28. Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
29. Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows, Vmware, Linux, których używa Zamawiający.
30. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Windows Server 2019/2022/2025 Vmware 8.0, Vmware 9.0, CentOS, których używa Zamawiający.
31. Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.
32. Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.
33. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
34. Macierz dyskowa musi zostać objęta minimum 3 letnim okresem gwarancji producenta z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
35. Zgłoszenia usterek muszą być akceptowane zarówno drogą email (w ofercie należy podać dedykowany adres email do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.).
36. Usługi gwarancyjne świadczone przez wykonawcę/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001:2008 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001:2008 lub równoważny.
37. Moduły SSD mają być objęte gwarancją która po awarii modułu nie wymaga zwrotu wymienionego dysku do producenta lub partnera serwisowego -niesprawny dysk pozostaje u Zamawiającego.
38. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
    - bezpłatna możliwość aktualizacje firmware;
    - dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń;
    - dostęp do centrum pomocy technicznej producenta;

- otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware;
- otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

39. Montaż w szafie RACK w miejscu wyznaczonym przez Zamawiającego.
40. Podłączenie do sieci zasilania zgodnie z wytycznymi Zamawiającego.
41. Uruchomienie i weryfikacja poprawności działania.
42. Aktualizacja oprogramowania do wersji zalecanej przez producenta.
43. Integracja serwerów z macierzą dyskową.
44. Projektowanie i konfiguracja przestrzeni dyskowej.
45. Skonfigurowanie powiadomień.
46. Dokumentacja techniczna.

3. Biblioteka taśmowa – 1 sztuka, 3 lata gwarancji NBD
Wymagane minimalne parametry techniczne

1. Obudowa do zamontowania w szafie rack, maksymalnie 1U. Wbudowany czytnik kodów kreskowych. Dostarczony odpowiedni zestaw umożliwiający instalacje urządzenia w szafie rack.
2. Biblioteka powinna umożliwiać obsługę napędów LTO7/8/9. W chwili dostawy w bibliotece powinien być zainstalowany napęd LTO8 SAS.
3. Wraz z urządzeniem powinno być dostarczone odpowiednie okablowanie umożliwiające podłączenie napędu LTO8 SAS do serwera rack wyposażonego w porty SAS SFF-8644 Okablowanie powinno mieć przynajmniej 4m długości.
4. Liczba slotów LTO: Minimum 9, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów
5. W komplecie 5 sztuk taśm LTO8 wraz z kodami kreskowymi oraz 1 taśma czyszcząca
6. Zainstalowany minimum jeden zasilacz wystarczający do obsługi dostarczonej konfiguracji biblioteki w raz z kablem minimum 10A i mającym przynajmniej 4.3m długości, odpowiednim do podłączenia z PDU z wyjściem C13. Wymaga się dostarczenia także okablowania 2.8m, minimum 10A o zakończeniach C13 - CEE7-VII.
7. Interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD.
8. Obsługa SNMP.
9. Funkcjonalność szyfrowania backupowanych danych. Nie akceptuje się rozwiązań wykorzystujących w celu szyfrowania tylko i wyłącznie zewnętrzne aplikacje. Szyfrowanie musi opierać się o bibliotekę taśmową. Jeśli funkcjonalność szyfrowania jest oddzielnie licencjonowana, nie jest wymagane jej dostarczenie w momencie dostawy urządzenia.
10. Obsługa SSL.
11. Funkcjonalność kompresji danych z wykorzystaniem nośników LTO9 w stopniu przynajmniej 2.5:1 . Na potrzeby kompresji powinien być wykorzystywany algorytm LZ-1 lub mocniejszy.
12. Wsparcie dla aplikacji min. CommVault Simpana, Dell/EMC NetWorker, Arcserve Backup, ASG Time Navigator, IBM Spectrum Protect, Microsoft System Center Data Protection Manager, Quest NetVault, Veritas Backup Exec/NetBackup, Veeam
13. Montaż w szafie RACK w miejscu wyznaczonym przez Zamawiającego.
14. Podłączenie do sieci zasilania zgodnie z wytycznymi Zamawiającego.
15. Uruchomienie i weryfikacja poprawności działania.

4. Oprogramowanie do backupu – licencja wieczysta dla 10 instancji, ze wsparciem producenta na 1 rok, serwis NBD
Wymagane minimalne parametry techniczne

1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter.
2. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 500, - minimalna ocena z referencji 4,6.
3. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x, 8.x i 9.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne dla powyższych platform wirtualizacyjnych, chyba, że wyszczególniono inaczej
4. Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.8.x - 7.3, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.5 lub nowszy, Proxmox VE 8.2, 8.3, 8.4 lub 9.0 oraz Scale Computing HyperCore 9.4.32.218226 – 9.5.x.
5. 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, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
6. System backupowy musi mieć możliwość wdrożenia wszystkich komponentów (np. serwer backupowy, serwer pośredniczący, repozytorium) na platformach Windows oraz Linux.
7. System backupowy musi mieć mieć możliwość wdrożenia w oparciu o tzw. appliance zgodny z wytycznymi bezpieczeństwa DISA (Defense Information Systems Agency).
8. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
9. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
10. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
11. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć wiele wirtualnych puli pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej 20 pamięci masowych w pojedyńczej puli.
12. Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.
13. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage, IBM Cloud Storage, 11:11 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.
14. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
15. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania do backupu oraz odtwarzania obrazu maszyny wirtualnej.

16. 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).
17. Oprogramowanie musi umożliwiać tworzenie logicznie odseparowanych środowisk dla różnych organizacji/działów. Dodatkowo system musi wspierać kontrolę dostępu w oparciu o role (RBAC) - predefiniowane lub własne.
18. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
19. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
20. 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.
21. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
22. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.
23. Oprogramowanie musi umożliwiać integracje z różnymi dostarczycielami tożsamości (IdP - Identity Providers) z wykorzystaniem protokołu SAML (np. Entra ID, Okta).
24. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora, reset zablokowanego konta).
25. Oprogramowanie musi posiadać integracje z systemami typu SIEM.
26. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
27. Oprogramowanie musi pozwalać na wydawanie komend głosowych asystentowi AI
28. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
29. 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 conajmniej dla platformy VMware i Hyper-V.
30. 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.
31. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
32. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
33. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
34. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
35. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 - 2025 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
36. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

37. 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.
38. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere lub dowolnego systemu operacyjnego Windows Server 2016-2025 (z innych platfrom - fizycznych, wirtualnych, chmurowych). Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
39. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
40. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
41. 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.
42. Dodatkowo dla środowiska vSphere, Hyper-V, Nutanix AHV i MS Azure powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
43. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w platformę. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
44. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny, zarówno fizycznej jak i wirtualnej.
45. 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.
46. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
47. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
48. 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.
49. 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.
50. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.
51. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.
52. Oprogramowanie musi wspierać bezagentowy backup, spójny aplikacyjnie (tzw. Application Consistent) dla maszyn wirtualnych z platfrom vSphere, Hyper-V, Nutanix AHV, Proxmox.

53. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej (Minimum dla Active Directory, MS Exchange, MS SQL, MS Sharepoint, Oracle i PostgreSQL).
54. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects oraz pozwalać na odtworzenie haseł.
55. Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications, Conditional Access Policies, Intune Policies.
56. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
57. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
58. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
59. 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.
60. 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.
61. Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
62. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.
63. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
64. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.
65. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.
66. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.
67. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
68. 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).
69. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych.
70. 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.

71. 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.
72. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.
73. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.
74. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
75. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
76. Instalacja i konfiguracja oprogramowania do tworzenia kopii zapasowych.
77. Definiowanie harmonogramów i polityk tworzenia kopii zapasowych, weryfikacja poprawności wykonywania backupów i przywracania danych.
78. Projektowanie architektury systemu backupu, konfiguracja replikacji oraz procedur odzyskiwania danych.
79. Dokumentacja techniczna środowiska.

5. Przełącznik dostępowy – 2 sztuki, 1 rok gwarancji NBD
Wymagane minimalne parametry techniczne

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym u Zamawiającego rozwiązaniem Fortigate FG60F.
Do wyżej wymienionego urządzenia: FG60F o numerze seryjnym FGT60FTK23077113 Wykonawca dostarczy odnowienie licencji i serwisów w zakresie: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox realizowana inline, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres do 30.06.2026.

1. Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Budżet mocy dla portów PoE min.: 740 W.
- Maksymalny pobór mocy bez budżetu dla PoE: 160 W.
- Minimalny zakres temperatury pracy: 0-40°C.

2. Interfejsy sieciowe - wymagania minimalne

Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45. W tym porty PoE w ilości co najmniej: 48, zgodne ze standardem: 802.3af oraz 802.3at.
b) 4 porty 10 GE SFP+ obsadzone wkładkami

3. Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

4. Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

5.Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

6.Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania/ NAC

- Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

- Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
- Centralne zarządzanie konfiguracją urządzenia
- Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
- Centralne zarządzanie sieciami VLAN.
- Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
- Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
- Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
- Automatyczna detekcja i rekomendacje konfiguracji.
- Przesyłanie logów na zewnętrzny serwer syslog.
- Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- Obsługa białych i czarnych list adresów MAC.
- Wykrywanie aplikacji komunikujących się w sieci.

- Musi być możliwe redundantne połączenie z elementami zarządzającymi.
- W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

7. Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

8. Dodatkowo:

- Konfiguracja przełączników sieciowych.
- Utworzenie odseparowanych podsieci, w tym sieci dla gości z ograniczonym dostępem.
- Rekonfiguracja sieci bezprzewodowej w celu spełnienia wymogów bezpieczeństwa.
- Konfiguracja podsieci UTM, reguł filtrowania i polityk bezpieczeństwa w oparciu o zaporę ogniową.
- Zabezpieczenie dostępu do zasobów sieciowych.
- Dokumentacja techniczna.

IV. SPOSÓB PRZYGOTOWANIA I ZŁOŻENIA INFORMACJI

1. Informacje należy złożyć do **24.02.2026 r.** na formularzu ofertowym w następujący sposób:

a) elektronicznie na adres promocja@obsza.pl

b) osobiście lub listownie w formie oryginału na adres Urząd Gminy Obsza, Obsza 36, 23-413 Obsza, pokój nr 8

2. Ceny w informacji dotyczącej wartości zamówienia należy podać w walucie polskiej (PLN – polskich złotych).

3. Ceny w informacji dotyczącej wartości zamówienia musi obejmować wszystkie koszty, jakie poniesie Wykonawca w związku z realizacją przedmiotu zamówienia
4. Osobami upoważnionymi do kontaktów ze strony Zamawiającego jest Krzysztof Szpatuśko, adres email: promocja@obsza.pl, telefon: (84) 9 10 02
5. W celu zapewnienia porównywalności danych, Zamawiający zastrzega sobie prawo do kontaktowania się z Wykonawcami w celu uzupełnienia lub doprecyzowania złożonych propozycji.

V. KLAUZULA INFORMACYJNA – RODO

Zgodnie z art. 13 ust. 1 i 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Wójt Gminy Obsza, Obsza 36, 23-413 Obsza tel. 84 6891002; e-mail sekretariat@obsza.pl;
2. W sprawach związanych z przetwarzaniem danych osobowych można kontaktować się z Inspektorem ochrony danych osobowych: tel. 604521364; mail: biuro@myszkowiak.pl
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego prowadzonym w trybie przetargu podstawowego oraz w celu archiwizacji i przeprowadzanych kontroli;
4. Podstawę prawną przetwarzania danych osobowych stanowi ustawa Prawo zamówień publicznych. 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.
5. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18-19 oraz 74 -76 ustawy Pzp.
6. Pani/Pana dane osobowe będą przechowane, 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, oraz przez okres wynikający z przepisów szczególnych dotyczących archiwizacji. Okresy te dotyczą również Wykonawców, którzy złożyli oferty i nie zostały one uznane, jako najkorzystniejsze (nie zawarto z tymi Wykonawcami umowy).
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
8. Posiada Pani/Pan prawo:
   1) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   2) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych[1];
   3) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO[2];

[1] 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

[2] 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.

4) 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:
   1) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   2) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Obsza, dn. 16-02-2026 r. ……..……..

Podpis Kierownika Zamawiającego lub osoby upoważnionej

Załączniki:

1. Formularz wyceny cenowej.