

**Ogłoszenie o zamówieniu  
Dostawy  
Zakup i dostawa sprzętu informatycznego i oprogramowania do Urzędu Miasta  
i Gminy Nowa Dęba w ramach realizacji projektu grantowego „Cyfrowa Gmina“**

**SEKCJA I - ZAMAWIAJĄCY**

**1.1.) Rola zamawiającego**

Postępowanie prowadzone jest samodzielnie przez zamawiającego

**1.2.) Nazwa zamawiającego:** Gmina Nowa Dęba

**1.4) Krajowy Numer Identyfikacyjny:** REGON 830409548

**1.5) Adres zamawiającego**

**1.5.1.) Ulica:** Rzeszowska 3

**1.5.2.) Miejscowość:** Nowa Dęba

**1.5.3.) Kod pocztowy:** 39-460

**1.5.4.) Województwo:** podkarpackie

**1.5.5.) Kraj:** Polska

**1.5.6.) Lokalizacja NUTS 3:** PL824 - Tarnobrzeski

**1.5.7.) Numer telefonu:** 158462671

**1.5.8.) Numer faksu:** 158465137

**1.5.9.) Adres poczty elektronicznej:** gmina@nowadeba.pl

**1.5.10.) Adres strony internetowej zamawiającego:** <http://www.nowadeba.pl/>

**1.6.) Rodzaj zamawiającego:** Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

**1.7.) Przedmiot działalności zamawiającego:** Ogólne usługi publiczne

**SEKCJA II – INFORMACJE PODSTAWOWE**

**2.1.) Ogłoszenie dotyczy:**

Zamówienia publicznego

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

**2.3.) Nazwa zamówienia albo umowy ramowej:**

Zakup i dostawa sprzętu informatycznego i oprogramowania do Urzędu Miasta i Gminy Nowa Dęba w ramach realizacji projektu grantowego „Cyfrowa Gmina“

**2.4.) Identyfikator postępowania:** ocds-148610-0c41dbc8-6bc7-11ed-aea3-5a7c432eaced

**2.5.) Numer ogłoszenia:** 2022/BZP 00455880/01

**2.6.) Wersja ogłoszenia:** 01

**2.7.) Data ogłoszenia:** 2022-11-24 09:30

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

**2.9.) Numer planu postępowań w BZP:** 2022/BZP 00054157/10/P

**2.10.) Identyfikator pozycji planu postępowań:**

1.2.2 Zakup i dostawa sprzętu informatycznego i oprogramowania do Urzędu Miasta i Gminy Nowa Dęba w ramach realizacji projektu grantowego „Cyfrowa Gmina“

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

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

**2.15.) Nazwa projektu lub programu**

Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020

**2.16.) Tryb udzielenia zamówienia wraz z podstawą prawną**

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

### **SEKCJA III – UDOSTĘPNIANIE DOKUMENTÓW ZAMÓWIENIA I KOMUNIKACJA**

**3.1.) Adres strony internetowej prowadzonego postępowania**

<http://www.nowadeba.pl/bip/przetargi/>

**3.2.) Zamawiający zastrzega dostęp do dokumentów zamówienia:** Nie

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

**3.5.) Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami - adres strony internetowej:** W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu mini Portalu, który dostępny jest pod adresem: <https://miniportal.uzp.gov.pl/ePUAPu,dostępnegopodadresem:https://epuap.gov.pl/wps/portal> oraz poczty elektronicznej: [gmina@nowadeba.pl](mailto:gmina@nowadeba.pl); (nie dotyczy składania ofert). Adres strony internetowej postępowania <http://www.nowadeba.pl/bip/przetargi/>

**3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej:** Ofertę, oświadczenia, o których mowa w art. 125 ust. 1 p.z.p., podmiotowe środki dowodowe w tym oświadczenie, o którym mowa w art. 117 ust.

4p.z.p., zobowiązanie podmiotu udostępniającego zasoby, pełnomocnictwa sporządza się w postaci elektronicznej, w ogólnie dostępnych formatach danych, w szczególności w formatach .txt, .rtf, .pdf, .doc, .docx, .odt. Ofertę, a także oświadczenie o jakim mowa w Dziale X ust. 1 SWZ składa się, pod rygorem nie ważności, w formie elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym (podpis zaufany - składany za pomocą profilu zaufanego) lub podpisem osobistym (podpis osobisty składany za pomocą dowodu osobistego - edowodu). Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy: „Formularz złożenia, zmiany, wycofania oferty lub wniosku” i „Formularz do komunikacji” wynosi 150MB.

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

**3.12.) Oferta - katalog elektroniczny:** Nie dotyczy

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

polski

**3.15.) RODO (obowiązek informacyjny):** 1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „Rozporządzenie”, informuję, że:

- 1) Administratorem Pani/Pana danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Nowa Dęba jest Burmistrz Miasta i Gminy Nowa Dęba, adres: ul. Rzeszowska 3, 39-460 Nowa Dęba, tel. +48 15 846 26 71, adres e-mail: [gmina@nowadeba.pl](mailto:gmina@nowadeba.pl).
- 2) W Urzędzie Miasta i Gminy Nowa Dęba został wyznaczony Inspektor Ochrony Danych, adres: ul. Rzeszowska 3, 39-460 Nowa Dęba, tel. : +48 15 846 26 71, adres e-mail: [iod@nowadeba.pl](mailto:iod@nowadeba.pl).
- 3) Dane osobowe będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia publicznego.
- 4) Dane osobowe będą przetwarzane przez okres zgodnie z art. 78 ust. 1 i 4 ustawy z dnia z dnia 11 września 2019 r.– Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm.), zwanej dalej 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 obowiązywania umowy.
- 5) Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia w związku z przepisami PZP.
- 6) Odbiorcami Pani/Pana danych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 4 PZP.
- 7) Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach PZP, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z PZP.

W związku z ograniczoną liczbą znaków klauzula RODO w całkowitym brzmieniu znajduje się z dziale II SWZ

### **SEKCJA IV – PRZEDMIOT ZAMÓWIENIA**

**4.1.) Informacje ogólne odnoszące się do przedmiotu zamówienia.****4.1.1.) Przed wszczęciem postępowania przeprowadzono konsultacje rynkowe:** Nie**4.1.2.) Numer referencyjny:** IR.271.59.2022**4.1.3.) Rodzaj zamówienia:** Dostawy**4.1.4.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania:** Nie**4.1.8.) Możliwe jest składanie ofert częściowych:** Tak**4.1.9.) Liczba części:** 3**4.1.10.) Ofertę można składać na wszystkie części****4.1.11.) Zamawiający ogranicza liczbę części zamówienia, którą można udzielić jednemu wykonawcy:** Nie**4.1.13.) Zamawiający uwzględni aspekty społeczne, środowiskowe lub etykiety w opisie przedmiotu zamówienia:** Nie**4.2. Informacje szczegółowe odnoszące się do przedmiotu zamówienia:****Część 1****4.2.2.) Krótki opis przedmiotu zamówienia**

60 Licencji oprogramowania do szyfrowania wiadomości email technologią END TO END. Wsparcie techniczne i prawo do aktualizacji na 2 lata. Bazy reguł, sygnatur i zagrożeń phishing na 2 lata.

1. Oprogramowanie musi zapewnić funkcjonalność:

1.1. szyfrowanie algorytmem AES256 treści wiadomości,

1.2. szyfrowanie algorytmem AES256 załączników,

1.3. szyfrowanie algorytmem AES256 plików,

1.4. szyfrowanie algorytmem AES256 katalogów,

1.5. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego,

1.6. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe,

1.7. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego,

1.8. do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego,

1.9. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Ubuntu Desktop 20.04.3, Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0,

1.10. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki,

1.11. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,

1.12. opieczutowania każdej wysłanej wiadomości sygnaturą, która jednoznacznie wskazuje na jej oryginalność,

1.13. zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,

1.14. posiadania wewnętrznej bazy haseł, która umożliwia:

1.14.1. export haseł do pliku,

1.14.2. import haseł z pliku

1.14.3. generowania ponownie haseł w bazie

1.15. posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich,

1.16. posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym,

1.17. posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów,

1.18. pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows,

1.19. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,

1.20. zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,

1.21. wykrywania fałszywych emaili - Antiphishing,

1.22. wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,

1.23. wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,

1.24. wykrywanie niebezpiecznych dokumentów MS Office,

1.25. wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,

1.26. definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,

1.27. współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać

min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlenie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 2 razy w ciągu dnia,

1.28. alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc,

1.29. współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.

2. Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.

1. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.

2. Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.

3. Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.

Przeprowadzenie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001 lub uprawnienia równoważne przez 2

**4.2.6.) Główny kod CPV:** 30236000-2 - Różny sprzęt komputerowy

**4.2.7.) Dodatkowy kod CPV:**

48000000-8 - Pakiety oprogramowania i systemy informatyczne

**4.2.8.) Zamówienie obejmuje opcje:** Nie

**4.2.10.) Okres realizacji zamówienia albo umowy ramowej:** 14 dni

**4.2.11.) Zamawiający przewiduje wznowienia:** Nie

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

**4.3.) Kryteria oceny ofert:**

**4.3.1.) Sposób oceny ofert:** Cena (C) – waga kryterium 60 %;

2) Wydłużenie wsparcia technicznego i praw do aktualizacji oraz gwarancji (G) – waga kryterium 40 %.

**4.3.2.) Sposób określania wagi kryteriów oceny ofert:** Procentowo

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

**Kryterium 1**

**4.3.5.) Nazwa kryterium:** Cena

**4.3.6.) Waga:** 60,00

**Kryterium 2**

**4.3.4.) Rodzaj kryterium:** inne.

**4.3.5.) Nazwa kryterium:** Wydłużenie wsparcia technicznego i praw do aktualizacji oraz gwarancji

**4.3.6.) Waga:** 40,00

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

**Część 2**

**4.2.2.) Krótki opis przedmiotu zamówienia**

1 Oprogramowanie serwera zarządzania komputerami przy pomocy kontrolera domeny wsparcie techniczne i prawo do aktualizacji na 2 lata.

1. Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość zarządzania systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:

1.1. interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową i być w standardzie Windows METRO,

1.2. system powinien przed zalogowaniem do panelu zarządzającego informować

w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny,

1.3. serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS),

1.4. musi posiadać system antywirusowy,

- 1.5. możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3,
- 1.6. musi umożliwiać dostęp administratorów przez przeglądarkę WEB,
- 1.7. wbudowany firewall zarządzany przez przeglądarkę WEB,
- 1.8. przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB,
- 1.9. system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB,
- 1.10. system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB.
2. W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność:
  - 2.1. zarządzania do min. 60 użytkowników, grup,
  - 2.2. zarządzania do min. 60 komputerów,
  - 2.3. zarządzania do min. 60 urządzeń,
  - 2.4. zarządzania polisami GPO,
  - 2.5. obsługę profili użytkowników oraz profili mobilnych,
  - 2.6. obsługę do min. 110 jednoczesnych połączeń do serwera domeny,
  - 2.7. zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB,
  - 2.8. możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB,
  - 2.9. nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB,
  - 2.10. wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB,
  - 2.11. listy użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB,
  - 2.12. listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB,
  - 2.13. wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym,
  - 2.14. możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego,
  - 2.15. administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB,
  - 2.16. administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.
  - 2.17. administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny.
  - 2.18. zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administrator do kontrolera domeny) do urządzenia sprzętowego token,
  - 2.19. pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny,
  - 2.20. urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0,
  - 2.21. urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u,
  - 2.22. współpraca z klientami Windows 7,8,8.1,10 w wersji professional.
3. Licencja kontrolera domeny dla zamawianego serwera głównego i zapasowego musi umożliwiać:
  - 3.1. łatwe przenoszenie i uruchomienie kontrolera domeny pomiędzy zamawianym serwerem głównym i zapasowym,
  - 3.2. łatwe uruchomienie kontrolera domeny w trybie awaryjnym (w ograniczonej funkcjonalności) na dowolnym serwerze posiadanego przez zamawiającego na czas naprawy zamówionego serwera głównego lub zapasowego.
4. Oprogramowanie musi umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować:
  - 4.1. obsługę minimum cztero-rdzeniowego procesora,
  - 4.2. obsługę minimum 32GB RAM-u,
  - 4.3. obsługę vmware VMDK,
  - 4.4. obsługę minimum 10 instancji środowisk wirtualnych,
  - 4.5. zapis stanu maszyny wirtualnej tzw. snapshot,
  - 4.6. kopię stanu maszyny wirtualnej,
  - 4.7. emulację wielu urządzeń np. kart sieciowych, kontrolerów SAS,
  - 4.8. dynamiczną alokację pamięci na kontener danych,
  - 4.9. współpracę z kontrolerami SATA, SCSI,
  - 4.10. tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci,
  - 4.11. zarządzanie przez przeglądarkę WEB,
  - 4.12. archiwizację uruchomionych maszyn wirtualnych.
5. Oprogramowanie musi również umożliwiać migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows Vista,7,8,8.1,10 w wersji 32 i 64 bity w wersji professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 110 użytkowników i musi realizować:
  - 5.1. automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego,
  - 5.2. automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL,
  - 5.3. automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego,
  - 5.4. automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego.

## 2 Specyfikacja wdrożenia:

1 Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami:

1.1 jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013

i Audytora Wewnętrznego ISO 14001 i 50001 lub uprawnienia równoważne,

1.2 jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013

i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne.

2 W ramach wdrożenia wykonawca przeszkoli kadrę informatyczną Urzędu z wdrożonych rozwiązań. Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne.

3 Wdrożenie i szkolenie z oprogramowania musi być realizowane przez certyfikowanych inżynierów z uprawnieniami wystawionymi przez producenta.

3

### Serwer główny:

1. Obudowa: RACK 1U.

2. Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie [http://www.cpubenchmark.net/high\\_end\\_cpus.html](http://www.cpubenchmark.net/high_end_cpus.html).

Procesor z obsługą wirtualizacji.

3. Pamięć: min. 32GB dedykowane do pracy serwerowej.

4. 4 kieszenie HotSwap SATA3.

5. 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap.

6. 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap.

7. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s.

8. Wsparcie KVM przez LAN.

9. Panel przedni chroniący kluczem dostęp do dysków.

10. Czujnik otwarcia obudowy.

11. Komplet szyn montażowych w zestawie.

12. Gwarancja: 2 lata gwarancji producenta.

### Serwer zapasowy:

1. Obudowa: RACK 1U.

2. Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie [http://www.cpubenchmark.net/high\\_end\\_cpus.html](http://www.cpubenchmark.net/high_end_cpus.html).

Procesor z obsługą wirtualizacji.

3. Pamięć: min. 32GB dedykowane do pracy serwerowej.

4. 4 kieszenie HotSwap SATA3.

5. 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap.

6. 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap.

7. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s.

8. Wsparcie KVM przez LAN.

9. Panel przedni chroniący kluczem dostęp do dysków.

10. Czujnik otwarcia obudowy.

11. Komplet szyn montażowych w zestawie.

12. Gwarancja: 2 lata gwarancji producenta.

**4.2.6.) Główny kod CPV:** 30236000-2 - Różny sprzęt komputerowy

**4.2.7.) Dodatkowy kod CPV:**

48820000-2 - Serwery

**4.2.8.) Zamówienie obejmuje opcje:** Nie

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

**4.2.11.) Zamawiający przewiduje wznowienia:** Nie

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

## 4.3.) Kryteria oceny ofert:

**4.3.1.) Sposób oceny ofert:** Cena (C) – waga kryterium 60 %;

2) Wydłużenie wsparcia technicznego i praw do aktualizacji oraz gwarancji (G) – waga kryterium 40 %.

**4.3.2.) Sposób określania wagi kryteriów oceny ofert:** Procentowo

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

## Kryterium 1

**4.3.5.) Nazwa kryterium:** Cena

**4.3.6.) Waga:** 60,00

#### **Kryterium 2**

**4.3.4.) Rodzaj kryterium:** inne.

**4.3.5.) Nazwa kryterium:** Wydłużenie wsparcia technicznego i praw do aktualizacji oraz gwarancji

**4.3.6.) Waga:** 40,00

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

### **Część 3**

#### **4.2.2.) Krótki opis przedmiotu zamówienia**

1 60 szt. urządzeń autoryzacyjnych do systemu operacyjnego lub serwera kontrolera domeny - TOKEN. Wsparcie techniczne i prawo do aktualizacji na 2 lata.

1 Uwierzytelnienie użytkowników do systemu operacyjnego lub serwera kontrolera domeny przy pomocy dedykowanego urządzenia sprzętowego, monitorowania logów uwzględniające:

1.1 logowanie do systemu (kto, kiedy)

1.2 wylogowanie/zablokowanie systemu (kto, kiedy).

2 Użytkownik zanim dokona logowania do systemu operacyjnego przy pomocy urządzenia sprzętowego może wyświetlić zdefiniowaną przez administratora wewnętrzną PBI. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.

3 Użytkownik, który opuszcza stanowisko pracy będzie miał blokowany system operacyjny przez urządzenie sprzętowe.

4 Pamięć urządzenia sprzętowego musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego.

5 Możliwość autoryzacji do systemu operacyjnego lub kontrolera domeny dedykowanym PIN-em.

6 Możliwość nadawania indywidualnego kodu PIN do urządzenia autoryzacyjnego TOKEN dla konta użytkownika w systemie operacyjnym lub kontrolerze domeny.

7 Zastosowane urządzenie sprzętowe powinno umożliwiać przypisywanie konkretnego komputera do urządzenia sprzętowego.

8 Narzędzie sprzętowe musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0.

9 Urządzenie sprzętowe w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u.

10 Współpraca z klientami Windows 7,8,8.1,10.

11 Wdrożenie i szkolenie z oprogramowania i urządzeń autoryzacyjnych musi być realizowane przez certyfikowanych inżynierów z uprawnieniami wystawionymi przez producenta.

**4.2.6.) Główny kod CPV:** 30236000-2 - Różny sprzęt komputerowy

**4.2.7.) Dodatkowy kod CPV:**

32422000-7 - Elementy składowe sieci

**4.2.8.) Zamówienie obejmuje opcje:** Nie

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

**4.2.11.) Zamawiający przewiduje wznowienia:** Nie

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

#### **4.3.) Kryteria oceny ofert:**

**4.3.1.) Sposób oceny ofert:** Cena (C) – waga kryterium 60 %;

2) Wydłużenie wsparcia technicznego i praw do aktualizacji oraz gwarancji (G) – waga kryterium 40 %.

**4.3.2.) Sposób określania wagi kryteriów oceny ofert:** Procentowo

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

#### **Kryterium 1**

**4.3.5.) Nazwa kryterium:** Cena

**4.3.6.) Waga:** 60,00

#### **Kryterium 2**

**4.3.4.) Rodzaj kryterium:** inne.

**4.3.5.) Nazwa kryterium:** Wydłużenie wsparcia technicznego i praw do aktualizacji oraz gwarancji

**4.3.6.) Waga:** 40,00

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

## SEKCJA V - KWALIFIKACJA WYKONAWCÓW

**5.1.) Zamawiający przewiduje fakultatywne podstawy wykluczenia:** Tak

**5.2.) Fakultatywne podstawy wykluczenia:**

Art. 109 ust. 1 pkt 4

Art. 109 ust. 1 pkt 5

Art. 109 ust. 1 pkt 7

**5.3.) Warunki udziału w postępowaniu:** Nie

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

**5.6.) Wykaz podmiotowych środków dowodowych na potwierdzenie niepodlegania wykluczeniu:** 1) Oświadczenie 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 wraz z oświadczeniem potwierdzającym aktualność oświadczenia wstępnego na podstawie art. 125 ust. 1 Pzp – załącznik nr 4 do SWZ;

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

3) Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w ust. 4 pkt 2 (Odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej), składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury. Dokument, o którym mowa powyżej, powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.

5. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 4 pkt 2, zastępuje się je w całości lub części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy. Dokument, o którym mowa powyżej, powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.

**5.9.) Zamawiający przewiduje uzupełnienie przedmiotowych środków dowodowych:** Nie

## SEKCJA VI - WARUNKI ZAMÓWIENIA

**6.1.) Zamawiający wymaga albo dopuszcza oferty wariantowe:** Nie

**6.3.) Zamawiający przewiduje aukcję elektroniczną:** Nie

**6.4.) Zamawiający wymaga wadium:** Tak

**6.4.1) Informacje dotyczące wadium:**

1. Wykonawca zobowiązany jest do zabezpieczenia swojej oferty wadium w wysokości: 300,00 zł (słownie: trzysta złotych) dla części I zamówienia;

600,00 zł (słownie: sześćset złotych) dla części II zamówienia;

200,00 zł (słownie: dwieście złotych) dla części III zamówienia;

2. Wadium wnosi się przed upływem terminu składania ofert.

3. Wadium może być wnoszone w jednej lub kilku następujących formach:

1) pieniądzu – przelewem na konto zamawiającego w Banku PEKAO S.A.

Nr 88 1240 2744 1111 0010 7170 2040

2) gwarancjach bankowych;

3) gwarancjach ubezpieczeniowych;

4) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2020 r. poz. 299).



4. Wadium wnoszone w formie pieniężnej musi wpłynąć na rachunek bankowy Zamawiającego najpóźniej przed upływem terminu składania ofert.
5. Wadium wnoszone w formie poręczeń lub gwarancji powinno być złożone w oryginale i musi obejmować cały okres związania ofertą. W przypadku wniesienia wadium w formie gwarancji lub poręczenia koniecznym jest, aby gwarancja lub poręczenie obejmowały odpowiedzialność za wszystkie przypadki powodujące utratę wadium, określone w art. 98 ust. 6 p.z.p.
6. Wadium w formie poręczeń lub gwarancji należy złożyć wraz z ofertą w oryginale w postaci elektronicznej.
7. Zasady zwrotu oraz okoliczności zatrzymania wadium określa art. 98 p.z.p.

**6.5.) Zamawiający wymaga zabezpieczenia należytego wykonania umowy: Tak**

**6.6.) Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:**

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Dziale X ust. 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.
4. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wraz z ofertą składają oświadczenie z którego wynika, które usługi/roboty wykonają poszczególni wykonawcy - Wzór oświadczenia stanowi załącznik nr 10 do SWZ.

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

**SEKCJA VII - PROJEKTOWANE POSTANOWIENIA UMOWY**

**7.1.) Zamawiający przewiduje udzielenia zaliczek: Nie**

**7.3.) Zamawiający przewiduje zmiany umowy: Tak**

**7.4.) Rodzaj i zakres zmian umowy oraz warunki ich wprowadzenia:**

1. Strony dopuszczają możliwość zmiany postanowień Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy w następujących przypadkach:
  - 1) zmiany terminu realizacji przedmiotu umowy, w następstwie:
    - a) siły wyższej - rozumianej jako wystąpienie zdarzenia nadzwyczajnego, zewnętrznego, niemożliwego do przewidzenia i zapobieżenia, którego nie dało się uniknąć nawet przy zachowaniu najwyższej staranności, a które uniemożliwia Wykonawcy wykonanie przedmiotu umowy. W razie wystąpienia siły wyższej Strony umowy zobowiązane są dołożyć wszelkich starań w celu ograniczenia do minimum opóźnienia w wykonywaniu swoich zobowiązań umownych, powstałego na skutek działania siły wyższej. (Pod pojęciem siły wyższej rozumie się w szczególności zdarzenia i okoliczności takie jak: klęska żywiołowa, działania wojenne, rebelie, terroryzm, rewolucja, powstanie, inwazja, bunt, zamieszki, strajk spowodowany przez inne osoby, niezwiązane z realizacją przedmiotu umowy, epidemia, itp.),
    - b) okoliczności leżących po stronie Zamawiającego i nie wynikających z przyczyn leżących po stronie Wykonawcy (np. wstrzymanie, zawieszenie, przerwa w realizacji),
    - c) przestojów i opóźnień zawinionych przez Zamawiającego,
    - d) wystąpienia okoliczności, których strony Umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności,
    - e) przyczyn niezależnych od którejkolwiek ze stron, które w szczególności dotyczyć będą: uwarunkowań formalno-prawnych;
  - 2) zmiany producenta lub modelu sprzętu (zastąpienie produktu lub rozszerzenie asortymentu o produkt równoważny lub wyższej jakości) w przypadku:
    - a) zaprzestania wytwarzania produktu objętego umową, w tym czasowego wstrzymania produkcji, pod warunkiem, iż odpowiednik jest tej samej lub wyższej jakości, za cenę nie wyższą niż cena produktu objętego umową,
    - b) wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, za cenę nie wyższą niż cena produktu objętego umową, wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, obok dotychczas oferowanego za cenę nie wyższą niż cena produktu objętego umową,
    - c) zmiany numeru katalogowego produktu, nazwy produktu, przy zachowaniu jego parametrów,
    - d) konieczności dokonania zmian w opisie niektórych elementów przedmiotu umowy, poprzez zastąpienie niektórych elementów sprzętem nowej generacji, z zastrzeżeniem zachowania ceny ofertowej.
  - 3) zmiana danych związana z obsługą administracyjno-organizacyjną umowy (danych teleadresowych Wykonawcy; Zamawiającego, zmiana rachunku bankowego) - zmiana ta następuje poprzez pisemne zgłoszenie tego faktu drugiej stronie i nie wymaga zawarcia aneksu do Umowy;
  - 4) przekształcenie Wykonawcy w związek z sukcesją generalną, przekształceniami, dziedziczeniem spółek handlowych zgodnie z KSH, a także sukcesją z mocy prawa, zgodnie z obowiązującymi przepisami (następstwa prawne) winno nastąpić w formie aneksu do Umowy.
2. Wszystkie powyższe postanowienia stanowią katalog zmian, na które Zamawiający może wyrazić zgodę. Nie stanowią

jednocześnie zobowiązania do wyrażenia takiej zgody.

3. W sytuacji wystąpienia okoliczności, o których wyżej mowa, każda ze stron może wystąpić z wnioskiem zawierającym:

- 1) opis propozycji zmiany, w tym wpływ na terminy wykonania;
- 2) uzasadnienie zmiany.

4. Wszelkie zmiany i uzupełnienia niniejszej Umowy dokonane w sposób zgodny z ustawą Pzp wymagają formy pisemnej pod rygorem nieważności - aneks do Umowy, z zastrzeżeniem przypadków określonych w niniejszym paragrafie, w których wskazano, że nie jest wymagane zawarcie aneksu do Umowy.

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

## **SEKCJA VIII – PROCEDURA**

**8.1.) Termin składania ofert:** 2022-12-20 09:00

**8.2.) Miejsce składania ofert:** Wykonawca składa ofertę za pośrednictwem „Formularza do złożenia, zmiany, wycofania oferty lub wniosku” dostępnego na ePUAP i udostępnionego również na miniPortalu. Funkcjonalność do zasyfrowania oferty przez Wykonawcę jest dostępna dla wykonawców na miniPortalu, w szczegółach danego postępowania.

**8.3.) Termin otwarcia ofert:** 2022-12-20 11:00

**8.4.) Termin związania ofertą:** do 2023-01-18