Ogłoszenie o wyniku postępowania
Dostawy
Zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego
Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: Gmina Osielsko

1.4) Krajowy Numer Identyfikacyjny: REGON 092350688

1.5) Adres zamawiającego

1.5.1.) Ulica: Szosa Gdańska 55A

1.5.2.) Miejscowość: Osielsko

1.5.3.) Kod pocztowy: 86-031

1.5.4.) Województwo: kujawsko-pomorskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL613 - Bydgosko-toruński

1.5.7.) Numer telefonu: 523241864

1.5.9.) Adres poczty elektronicznej: zampub@osielsko.pl

1.5.10.) Adres strony internetowej zamawiającego: www.bip.osielsko.pl

1.6.) Adres strony internetowej prowadzonego postępowania:
www.bip.osielsko.pl

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

1.8.) 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 komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina

2.4.) Identyfikator postępowania: ocds-148610-35f32b15-4ae8-11ed-8832-4e4740e186ac

2.5.) Numer ogłoszenia: 2022/BZP 00411778

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2022-10-26

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

2.9.) Numer planu postępowań w BZP: 2022/BZP 00019844/10/P

2.10.) Identyfikator pozycji planu postępowań:

1.2.3 Zakup sprzętu komputerowego w ramach projektu pn. Cyfrowa Gmina

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

2.12.) Nazwa projektu lub programu:

Program Operacyjny Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczące realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00

2.13.) Zamówienie/umowa ramowa było poprzedzone ogłoszeniem o zamówieniu/ogłoszeniem o zamiarze zawarcia umowy: Tak

2.14.) Numer ogłoszenia: 2022/BZP 00391422/01

SEKCJA III – TRYB UDZIELENIA ZAMÓWIENIA LUB ZAWARCIA UMOWY RAMOWEJ

3.1.) Tryb udzielenia zamówienia wraz z podstawą prawną Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Numer referencyjny: liZP.271.D.4.2022

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

4.4.) Rodzaj zamówienia: Dostawy

Część 1

4.5.1.) Krótki opis przedmiotu zamówienia
Część 1: Zakup macierzy dyskowej
Lp. Nazwa parametru Minimalna wartość parametru
1. Obudowa System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19"
2. Pojemność: System musi zostać dostarczony w konfiguracji zawierającej minimum:

12 dysków 4TB NL-SAS

oraz posiadać możliwość rozbudowy o kolejne dyski
System musi wspierać dyski:
• SAS: 900GB do 1800GB
• SATA/NL-SAS: od 4TB do 16TB
• SSD: 800GB do 7600GB
Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania/migrowania danych. (zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami).
Zamawiający dopuszcza rozwiązanie które nie pozwala na rozbudowę do wyższego modelu przy założeniu, że zostanie zaoferowany najwyższy model z rodziny z pamięcią Cache min 1TB na kontroler.
System musi mieć możliwość rozbudowy do 500 dysków w obrębie pary kontrolerów lub w obrębie klastra wielu kontrolerów (scale-out) w zależności od sposobu realizacji rozbudowy dla oferowanego rozwiązania.
W przypadku klastrowania kontrolerów macierzy, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, nie dopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego.
Dla rozwiązań wykorzystujących klastrowanie (scale-out) musi być możliwość rozbudowy rozwiązania do co najmniej 12 kontrolerów w klastrze.
Rozwiązanie musi pozwalać na rozbudowę o dyski lub kontrolery wykonane w technologii NVMe do min 550 dysków w technologii NVME. Zamawiający dopuszcza zaoferowanie rozwiązania, które nie posiada takiej możliwości w przypadku gdy całość zasobów zostanie dostarczona na dyskach flash/SSD.
3. Kontroler Dwa kontrolery wyposażone w przynajmniej 256GB cache każdy.

Zamawiający dopuszcza alternatywnie rozwiązanie posiadające co najmniej 32GB cache oparte o RAM na kontroler jeżeli dodatkowo zostanie dostarczona z macierzą dodatkowa pamięć Flash minimum 1024GB pamięci na kontroler (wbudowana w kontroler lub formie dodatkowych dysków Flash skonfigurowanych w RAID 10)

Procesory macierzy powinny być wykonane w technologii wielordzeniowej z przynajmniej 12 rdzeniami na każdy kontroler dla procesorów AMD i Intel. Dla innych rodzajów procesorów min 64 rdzenie.
W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub poprzez zrzut na pamięć nieulotną
Macierz musi pozwalać na poszerzenie pamięci Cache za pomocą dysków SSD do 6TB.
4. Interfejsy Oferowana macierz musi posiadać minimum

8 portów 10GbE sfp+
2 porty 1Gb do zarządzania
4 porty 12Gb SAS,

5. RAID System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID
6. Kopie Migawkowe Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/- 5%
7. Obsługiwane protokoły Macierz musi obsługiwać jednocześnie protokoły FC, iSCSi, CIFS i NFS, S3 (macierz obiektowa) - jeśli wymagane są licencje zamawiający wymaga dostarczenia ich wraz z macierzą.

8. Inne wymagania Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2003/2008, Linux, Vmware, Unix

Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie

Macierz musi posiadać funkcjonalność priorytetyzacji zadań.

Macierz musi posiadać funkcjonalność kompresji danych w trybie in-line oraz off-line na każdym rodzaju danych.

Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie. Jeżeli oferowane rozwiązanie nie posiada funkcjonalności deduplikacji danych, zamawiający wymaga dostarczenia 4-krotności przestrzeni wyspecyfikowanej.

Macierz musi posiadać funkcjonalność replikacji synchronicznej i asynchronicznej pomiędzy macierzami tego samego producenta. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów.
Zamawiający dopuszcza zastosowanie zewnętrznego wirtualizatora (po 1 szt na replikowaną macierz) w celu spełnienia możliwości replikacji danych.

System musi pozwalać na rozbudowę o specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności:
- musi informować administratora w przypadku nie standardowego zachowania systemu oraz danych
- wykonywać prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware

Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy.

Macierz musi posiadać funkcjonalność wykonania wirtualnych klonów, które nie wymagają kopiowania bloków danych.

Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na:
- monitoring wykorzystania przestrzeni na macierzy
- monitoring grup RAIDowych
- monitoring wykonywanych backupów/replikacji danych między macierzami
- monitoring wydajności macierzy
- analizę i diagnozę spadku wydajności
Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność macierzy.

Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy

Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności:
a) Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego.
- procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta.
- procedura musi uwzględniać systemy zależne np, macierze replikujące
- procedura musi umożliwiać generowanie planu cofnięcia aktualizacji.
b) Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnościom macierzy.
c) Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji.

Portal lub oprogramowanie może pochodzić od innego producenta niż producent macierzy, z tym że zostanie dostarczona odpowiednia licencja do maksymalnej pojemności macierzy.

Zamawiający wymaga by wszystkie funkcjonalności działały wspólnie tj. włączenie jednej funkcjonalności nie eliminowało

innej.

9. Gwarancja i serwis 3 lata serwisu producenta z 2 godzinnym czasem odpowiedzi na awarie krytyczne i dostawą elementów w na następny dzień roboczy

Zepsute dyski pozostają u zamawiającego

Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.

10. Macierz musi posiadać funkcjonalność „Tieringu" zimnych danych na:
- inną macierz tego samego producenta (z wolnymi dyskami np. NL-SAS)
- inną macierz dowolnego producenta z protokołem S3
- Tiering musi być natywnym narzędziem macierzy i wykonywać się automatycznie.

4.5.3.) Główny kod CPV: 30233000-1 - Urządzenia do przechowywania i odczytu danych

4.5.5.) Wartość części: 48780,49 PLN

Część 2

4.5.1.) Krótki opis przedmiotu zamówienia
Część 2: Zakup urządzenia UTM
OBSŁUGA SIECI
1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
INTRUSION PREVENTION SYSTEM (IPS)
12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
20. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET,

SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
KSZTAŁTOWANIE PASMA (Traffic Shapping)
21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA
25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
OCHRONA ANTYSPAM
29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
a. białe/czarne listy,
b. DNS RBL,
c. Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)
33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
a. PPTP VPN,
b. IPSec VPN,
c. SSL VPN.
35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
FILTR DOSTĘPU DO STRON WWW
40. Urządzenie ma posiadać wbudowany filtr URL.
41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
42. Administrator ma mieć możliwość dodawania własnych kategorii URL.
43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
a. blokowanie dostępu do adresu URL,
b. zezwolenie na dostęp do adresu URL,
c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
47. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
UWIERZYTELNIANIE
49. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
a. lokalną bazę użytkowników (wewnętrzny LDAP),
b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
c. usługę katalogową Microsoft Active Directory.
50. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
51. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
a. SSL,
b. Radius,

c. Kerberos.
52. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
53. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)
55. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
a. równoważenie względem adresu źródłowego,
b. równoważenie względem połączenia.
57. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
58. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
59. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
60. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
61. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

62. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
63. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
64. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
65. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
ADMINISTRACJA URZĄDZENIEM
66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
67. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
ciąg dalszy SWZ cz. II str. 9-11

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

4.5.5.) Wartość części: 13821,14 PLN

Część 3

4.5.1.) Krótki opis przedmiotu zamówienia
Część 3: Zakup i dostawa oprogramowania z licencją na Backup na 3 serwery fizyczne (w tym 6 virtrualnych), oraz 40 stacji roboczych

Wymagana funkcjonalność oprogramowania do Backup stacji roboczych:

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Produkt z licencją dożywotnią
3. Aktualizacja oprogramowania na min 1 rok
4. Wsparcie dla systemów operacyjnych Windows typu stacja robocza:
Systemy operacyjne Windows: Windows 8/8.1, Windows XP, Windows Vista, Windows 7, Windows 10, Windows 11
5. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
6. Tworzenie kopii zapasowych dysków/partycji
7. Tworzenie kopii zapasowych plików i folderów
8. Replikacja kopii zapasowych do wielu lokalizacji docelowych
9. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
10. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
11. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD
12. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
13. Zdalna instalacja i aktualizacja agentów na komputerach klienckich
14. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
15. Obsługa napędów taśmowych.
16. Deduplikacja kopii zapasowych.
17. Możliwość generowania planu przywracania kopii zapasowych
18. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach
19. Szablony schematów rotacji kopii zapasowych
20. Polecenia poprzedzające/następujące
21. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)

22. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)
23. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
24. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
25. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
26. Pełne, przyrostowe i różnicowe kopie zapasowe
27. Wysyłanie powiadomień pocztą e-mail
28. Szyfrowane kopii zapasowych algorytmem AES
29. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.
30. Funkcjonalność ciągłej ochrony danych
31. Analiza podatności urządzenia (poszukiwanie luk w oprogramowaniu objętym ochroną), środowisko Windows
32. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem.
33. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
34. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
35. Uruchamianie usług z minimalnymi prawami użytkownika
36. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
37. Pomoc techniczna dostępna w języku polskim
38. Administrowanie kontami użytkowników aplikacji
39. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain
40. Wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków
41. Migawki wielowoluminowe
42. Kopia zapasowa „sektor po sektorze"
43. Obsługa dysków dynamicznych

Wymagana funkcjonalność oprogramowania do Backup Serwerów:

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Wsparcie dla środowisk wirtualizacji: Hyper-V, VMware vSphere, Citrix XenServer, Red Hat Virtualization, Linux KVM I Oracle VM Server
3. Obsługa aplikacji MS SQL, MS Exchange, AD, SharePoint, BD Oracle,
4. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
5. Obsługa środowiska chmurowego
6. Tworzenie kopii zapasowych dysków/partycji
7. Tworzenie kopii zapasowych plików i folderów
8. Replikacja kopii zapasowych do wielu lokalizacji docelowych
9. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
10. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
11. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD
12. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
13. Zdalna instalacja i aktualizacja agentów na komputerach klienckich
14. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
15. Obsługa napędów taśmowych.
16. Deduplikacja kopii zapasowych.
17. Możliwość generowania planu przywracania kopii zapasowych
18. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach
19. Szablony schematów rotacji kopii zapasowych
20. Polecenia poprzedzające/następujące
21. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)
22. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)
23. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
24. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
25. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
26. Pełne, przyrostowe i różnicowe kopie zapasowe
27. Wysyłanie powiadomień pocztą e-mail
28. Szyfrowane kopii zapasowych algorytmem AES
29. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.
30. Funkcjonalność ciągłej ochrony danych
31. Analiza podatności urządzenia (poszukiwanie luk w oprogramowaniu objętym ochroną), środowisko Windows

Funkcjonalność unikalna:

32. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem.
33. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
34. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
35. Uruchamianie usług z minimalnymi prawami użytkownika
36. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
37. Pomoc techniczna dostępna w języku polskim
38. Administrowanie kontami użytkowników aplikacji
39. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain

4.5.3.) Główny kod CPV: 72268000-1 - Usługi dostawy oprogramowania

4.5.5.) Wartość części: 9956,10 PLN

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA

Część 1

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 1)

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 2 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Zgodnie z treścią art. 255 pkt. 2 ustawy Prawo zamówień publicznych, Zamawiający unieważnia postępowanie o udzielenie zamówienia, jeżeli wszystkie złożone wnioski o dopuszczenie do udziału w postępowaniu albo oferty podlegały odrzuceniu. W ww. postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie podstawowym Zamawiający odrzucił wszystkie oferty, w związku z czym unieważnia postępowania zgodnie z art. 255 pkt 2 ustawy Pzp.

Uzasadnienie wyboru
Zamawiający działając zgodnie z art. 226 ust. 1 pkt 5 ustawy Prawo zamówień publicznych (t. j. Dz. U. z 2022 r. poz. 1710 ze zm.) odrzucił ofertę ANZENA Sp. z o.o. ul. Pszczyńska 15, 40-478 Katowice, ponieważ jej treść jest niezgodna z warunkami zamówienia.
Wykonawca w ofercie podał 45 dniowy termin realizacji dostawy. Zamawiający, zgodnie z zapisami SWZ - część XV pkt. B, wymagał wskazania terminu dostawy wynoszącego 30, 40 lub 60 dni, będącego kryterium oceny ofert. W związku z powyższym oferta ww. Wykonawcy podlega odrzuceniu.

Część 2

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 2)

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 3 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Działając na podstawie art. 255 pkt 3 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2022 r., poz. 1710 ze zm.) Zamawiający informuje, że unieważnia postępowanie prowadzone w trybie podstawowym na podstawie art. 275 pkt 1, ponieważ oferta z najniższą ceną przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia.

Uzasadnienie wyboru
Zgodnie z treścią art. 255 pkt. 3 ustawy Prawo zamówień publicznych, Zamawiający unieważnia postępowanie o udzielenie zamówienia, jeżeli cena lub koszt najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba że zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty.
Zamawiający, stosownie do art. 222 ust. 4 ustawy Pzp, przed terminem otwarciem ofert udostępnił na stronie internetowej prowadzonego postępowania kwotę, jaką zamierza przeznaczyć na sfinansowanie przedmiotowego zamówienia tj. 20 000,00 zł brutto.
Po analizie możliwości finansowych jednostki, zamawiający stwierdził, iż w chwili obecnej nie jest możliwe zwiększenie kwoty pierwotnie przeznaczonej na realizację zamówienia do ceny oferty z najniższą ceną. W związku z powyższym

Zamawiający unieważnia postępowanie.

Część 3

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 3)

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 2 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Zgodnie z treścią art. 255 pkt. 2 ustawy Prawo zamówień publicznych, Zamawiający unieważnia postępowanie o udzielenie zamówienia, jeżeli wszystkie złożone wnioski o dopuszczenie do udziału w postępowaniu albo oferty podlegały odrzuceniu. W ww. postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie podstawowym Zamawiający odrzucił wszystkie oferty, w związku z czym unieważnia postępowania zgodnie z art. 255 pkt 2 ustawy Pzp.
Uzasadnienie odrzucenia
Zamawiający działając zgodnie z art. 226 ust. 1 pkt 5 ustawy Prawo zamówień publicznych (t. j. Dz. U. z 2022 r. poz. 1710 ze zm.) odrzucił ofertę HOTKEY404 Tomasz Tańcula, ponieważ jej treść jest niezgodna z warunkami zamówienia. Wykonawca w ofercie podał 7 dniowy termin realizacji dostawy. Zamawiający, zgodnie z zapisami SWZ - część XV pkt. B, wymagał wskazania terminu dostawy wynoszącego 30, 40 lub 60 dni, będącego kryterium oceny ofert. W związku z powyższym oferta ww. Wykonawcy podlega odrzuceniu.

Zamawiający informuje, że na podstawie art. 226 ust. 1 pkt 3 ustawy Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm.) odrzucił ofertę HOTKEY404 Tomasz Tańcula, jako niezgodną z przepisami ustawy, tj. z art. 63.
Oferta została przekazana przy użyciu środków komunikacji elektronicznej, określonymi przez Zamawiającego w SWZ, bez podpisu Wykonawcy.
Kwestie związane z opatrywaniem ofert podpisem elektronicznym reguluje art. 63 ustawy Pzp. Zgodnie z ww. przepisem w postępowaniu o udzielenie zamówienia o wartości mniejszej niż progi unijne ofertę składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Wykonawca przekazuje zamawiającemu zaszyfrowany plik zawierający ofertę opatrzoną właściwym podpisem lub plik oferty wraz z plikiem podpisu (w przypadku podpisu zewnętrznego), przy czym opatrzenie oferty podpisem nastąpiło przed jej zaszyfrowaniem. Dopuszczalne jest również, aby wykonawca przekazał zamawiającemu swoją ofertę w tzw. „paczce" dokumentów elektronicznych (tj. w skompresowanym archiwum dokumentów elektronicznych) wraz z właściwym podpisem dołączonym jako plik podpisu do paczki dokumentów elektronicznych przed jej zaszyfrowaniem, o czym wprost stanowi § 8 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r., poz. 2452).
W postępowaniu o udzielenie zamówienia publicznego prowadzonym przez Zamawiającego składanie ofert odbywa się za pośrednictwem miniPortal/ePUAP. Przekazanie oferty następuje za pomocą „formularza złożenia, zmiany, wycofania oferty". Formularz ten może być przed wysłaniem podpisany przez użytkownika (podpis następuje z wykorzystaniem właściwej funkcji systemu ePUAP tj. „PODPISZ I WYŚLIJ"). Podnieść należy, że podpis ten składany jest wyłącznie na „formularzu do złożenia, zmiany, wycofania oferty". Co za tym idzie, podpis na formularzu to jedynie funkcjonalność systemu ePuap, z której mogą, ale nie muszą skorzystać wykonawcy przekazujący ofertę przy pomocy tego systemu. Podpis złożony jedynie na ww. formularzu nie może wywierać skutków w odniesieniu do złożonej za jego pomocą oferty wykonawcy. Oferta, zgodnie z art. 63 ustawy Pzp, a nie formularz elektroniczny za pośrednictwem którego jest przekazywana, musi zostać opatrzona właściwym podpisem. Oferta złożona za pośrednictwem środków komunikacji elektronicznej powinna zostać opatrzona właściwym podpisem przed jej zaszyfrowaniem. Złożenie podpisu jedynie w innym miejscu nie jest równoznaczne ze złożeniem podpisu pod ofertą.
Oferta Wykonawcy HOTKEY404 Tomasz Tańcula została złożona bez opatrzenia jej właściwym podpisem elektronicznym i podlega odrzuceniu na podstawie art. 226 ust. 1 pkt 3 ustawy Pzp z uwagi na niezgodność z art. 63 ustawy Pzp.