

**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: 52 324 18 64

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-a68cd457-6674-11ed-aea3-5a7c432eaced

2.5.) Numer ogłoszenia: 2022/BZP 00520887

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2022-12-29

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

2.9.) Numer planu postępowań w BZP: 2022/BZP 00019844/12/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 00444569/01

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.5.2022

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

Przedmiotem zamówienia jest zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina, według poniższych specyfikacji:

Część 1: Zakup macierzy dyskowej

Nazwa parametru Minimalna wartość parametru

Obudowa Do instalacji w standardowej szafie RACK 19", macierz musi zajmować maksymalnie 2U i pozwalać na instalację 12 dysków 3.5".

Kontrolery Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 25Gb iSCSI w Standardzie Sfp+/SFP28

Dołączone minimum dwa transmiery optyczne SFP+ 10Gb SR

Cache 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.

Dyski Zainstalowane:

5 dysków Hot-Plug o pojemności 4TB SAS 12Gbps 3,5",

Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 264 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.

Oprogramowanie/

Funkcjonalności Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5.

Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz.

Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków.

Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.

Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.

Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.

Wsparcie dla systemów operacyjnych Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, VMware ESXi, Citrix XenServer

Bezpieczeństwo Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.

Warunki gwarancji dla macierzy 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.

Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygasnięcia gwarancji macierzy.

Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.

Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.

W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

Dokumentacja użytkownika Zamawiający wymaga dokumentacji w języku polskim lub angielskim

Certyfikaty Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015.

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

Przedmiotem zamówienia jest zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina, według poniższych specyfikacji:

Część 2: Zakup urządzenia UTM

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 8 portami Gigabit Ethernet RJ-45.
- 2 gniazdami SFP 1 Gbps.

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB.

5. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.

4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.

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

Polityki, Firewall

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

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łącz WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routing (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

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

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
- ciąg dalszy zgodnie z SWZ cz. II str. 7 -10

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

Przedmiotem zamówienia jest zakup i dostawa sprzętu komputerowego wraz z oprogramowaniem dla Urzędu Gminy w Osielsku w ramach projektu pn. Cyfrowa Gmina, według poniższych specyfikacji:

Część 3: Zakup i dostawa oprogramowania z licencją na Backup na 6 serwerów wirtualnych oraz 5 stacji roboczych

Wymagania do oprogramowania do Backupu dla 5 komputerów, 6 wirtualnych serwerów, licencje bezterminowe

1. Pełne wsparcie dla systemów rodziny Microsoft Windows Server: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Storage Server 2012 R2 Essentials, Windows Server 2008 R2 Foundation, Windows Server 2008 Foundation z SP2 lub wyższy, Windows Server 2003, Windows Server 2003 R2, Windows 2000 Server/Advanced Server (SP4 lub nowszy),
2. Pełne wsparcie dla systemów rodziny Windows Small Business Server: Windows Server 2012 R2 (Essentials, Foundation), Windows Server 2012 (Essentials, Foundation), Windows Small Business Server 2011, Windows Small Business Server 2008 (Standard i Premium), Windows Server 2008 R2 Foundation, Windows Small Business Server 2003 i R2
3. Pełne wsparcie dla środowisk wirtualnych: VMware Workstation, VMware ESX/ESXi, Microsoft Hyper-V, Microsoft Virtual PC, Microsoft Virtual Server, Oracle VirtualBox, Citrix XenServer, Linux KVM, ProxMox, Red Hat Enterprise Virtualization (RHEV), Stratos everRun.
4. Wsparcie dla 32 i 64-bitowych systemów Microsoft.
5. Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS.
6. Wsparcie dla dysków z tablicą partycji MBR oraz GPT
7. Pełne wsparcie dla systemów Ubuntu 14.04, 16.04, 18.04, CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Oracle Linux (wszystkie systemy 64-bitowe).
8. Wsparcie systemów plików: ext2, ext3, ext4, XFS.
9. Program i wsparcie techniczne dostępne w języku polskim
10. Wsparcie dla 32 i 64-bitowych systemów Microsoft: Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10.

Tworzenie kopii zapasowych (backupu)

1. Backup obejmuje kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami.
2. Program umożliwia skonfigurowanie różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umożliwiać backup z częstotliwością min. co 15 minut.
3. Istnieje możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski

USB, Firewall.

4. Program wykonuje kopie zapasowe (backupy) na poziomie sektorów czyli backup przyrostowy zawiera tylko zmienione sektory na dysku a nie np. całe pliki.
5. Program nie wymaga oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny jest przechowywany bezpośrednio na tej maszynie.
6. Możliwe jest tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g.
7. Do wykonywania kopii zapasowej wykorzystywana jest technologia Microsoft VSS oraz certyfikowany sterownik Microsoftu.
8. Program umożliwia wykonywanie kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive'a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego.
9. Rozwiązanie pozwala na okresową weryfikację, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać.
10. Rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi.
11. Podczas tworzenia kopii zapasowej program generuje plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu.
12. Program posiada narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email.
13. Program umożliwia konwersję kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX.
14. Program umożliwia replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP.

Przywracanie z kopii zapasowych

15. Możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive'a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu.
16. Program pozwala na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej, oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną.
17. Bez względu na rozmiar backupu, program umożliwia automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMware vSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej.
18. Program umożliwia zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości.
19. Podczas przywracania obrazu dysku/partycji z kopii zapasowej, program umożliwia: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows.
20. Program pozwala na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni.

Zdalne zarządzanie

21. Program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej.
22. Musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej.
23. Konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych.
24. Konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych.
25. Program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej.
26. Musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO.

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 zawarciem umowy

SEKCJA VI OFERTY (dla części 1)

6.1.) Liczba otrzymanych ofert lub wniosków: 1

6.1.3.) Liczba otrzymanych od MŚP: 1

6.1.4.) Liczba ofert wykonawców z siedzibą w państwach EOG innych niż państwo zamawiającego: 0

6.1.5.) Liczba ofert wykonawców z siedzibą w państwie spoza EOG: 0

6.1.6.) Liczba ofert odrzuconych, w tym liczba ofert zawierających rażąco niską cenę lub koszt: 0

6.1.7.) Liczba ofert zawierających rażąco niską cenę lub koszt: 0

6.2.) Cena lub koszt oferty z najniższą ceną lub kosztem: 51364,80 PLN

6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 51364,80 PLN

6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 51364,80 PLN

6.5.) Do wyboru najkorzystniejszej oferty zastosowano aukcję elektroniczną: Nie

6.6.) Oferta wybranego wykonawcy jest ofertą wariantową: Nie

SEKCJA VII WYKONAWCA, KTÓREMU UDZIELONO ZAMÓWIENIA (dla części 1)

7.1.) Czy zamówienie zostało udzielone wykonawcom wspólnie ubiegającym się o udzielenie zamówienia: Nie

Wykonawca

7.2.) Wielkość przedsiębiorstwa wykonawcy: Mikro przedsiębiorca

7.3.) Dane (firmy) wykonawcy, któremu udzielono zamówienia:

7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia: 4ITS Jacek Lange

7.3.2) Krajowy Numer Identyfikacyjny: 8491268028

7.3.4) Miejscowość: Bydgoszcz

7.3.6.) Województwo: kujawsko-pomorskie

7.3.7.) Kraj: Polska

7.3.8.) Czy wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcom?: Nie

SEKCJA VIII UMOWA (dla części 1)

8.1.) Data zawarcia umowy: 2022-12-28

8.2.) Wartość umowy/umowy ramowej: 51364,80 PLN

8.3.) Okres realizacji zamówienia albo umowy ramowej: 14 dni

Część 2

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 2)

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

SEKCJA VI OFERTY (dla części 2)

6.1.) Liczba otrzymanych ofert lub wniosków: 2

6.1.3.) Liczba otrzymanych od MŚP: 2

6.1.4.) Liczba ofert wykonawców z siedzibą w państwach EOG innych niż państwo zamawiającego: 0

6.1.5.) Liczba ofert wykonawców z siedzibą w państwie spoza EOG: 0

6.1.6.) Liczba ofert odrzuconych, w tym liczba ofert zawierających rażąco niską cenę lub koszt: 0

- 6.1.7.) Liczba ofert zawierających rażąco niską cenę lub koszt: 0
- 6.2.) Cena lub koszt oferty z najniższą ceną lub kosztem: 17664,18 PLN
- 6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 19803,00 PLN
- 6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 17664,18 PLN
- 6.5.) Do wyboru najkorzystniejszej oferty zastosowano aukcję elektroniczną: Nie
- 6.6.) Oferta wybranego wykonawcy jest ofertą wariantową: Nie

SEKCJA VII WYKONAWCA, KTÓREMU UDZIELONO ZAMÓWIENIA (dla części 2)

- 7.1.) Czy zamówienie zostało udzielone wykonawcom wspólnie ubiegającym się o udzielenie zamówienia: Nie

Wykonawca

- 7.2.) Wielkość przedsiębiorstwa wykonawcy: Mikro przedsiębiorca
- 7.3.) Dane (firmy) wykonawcy, któremu udzielono zamówienia:
- 7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia: 4ITS Jacek Lange
- 7.3.2) Krajowy Numer Identyfikacyjny: 8491268028
- 7.3.4) Miejscowość: Bydgoszcz
- 7.3.6.) Województwo: kujawsko-pomorskie
- 7.3.7.) Kraj: Polska
- 7.3.8.) Czy wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcom?: Nie

SEKCJA VIII UMOWA (dla części 2)

- 8.1.) Data zawarcia umowy: 2022-12-28
- 8.2.) Wartość umowy/umowy ramowej: 17664,18 PLN
- 8.3.) Okres realizacji zamówienia albo umowy ramowej: 14 dni

Część 3

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA (dla części 3)

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

SEKCJA VI OFERTY (dla części 3)

- 6.1.) Liczba otrzymanych ofert lub wniosków: 2
- 6.1.1.) Liczba otrzymanych ofert wariantowych: 0
- 6.1.2.) Liczba ofert dodatkowych: 0
- 6.1.3.) Liczba otrzymanych od MŚP: 2
- 6.1.4.) Liczba ofert wykonawców z siedzibą w państwach EOG innych niż państwo zamawiającego: 0
- 6.1.5.) Liczba ofert wykonawców z siedzibą w państwie spoza EOG: 0
- 6.1.6.) Liczba ofert odrzuconych, w tym liczba ofert zawierających rażąco niską cenę lub koszt: 0
- 6.1.7.) Liczba ofert zawierających rażąco niską cenę lub koszt: 0
- 6.2.) Cena lub koszt oferty z najniższą ceną lub kosztem: 6124,17 PLN
- 6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 16641,90 PLN
- 6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 6124,17 PLN
- 6.5.) Do wyboru najkorzystniejszej oferty zastosowano aukcję elektroniczną: Nie
- 6.6.) Oferta wybranego wykonawcy jest ofertą wariantową: Nie

SEKCJA VII WYKONAWCA, KTÓREMU UDZIELONO ZAMÓWIENIA (dla części 3)

7.1.) Czy zamówienie zostało udzielone wykonawcom wspólnie ubiegającym się o udzielenie zamówienia: Nie

Wykonawca

7.2.) Wielkość przedsiębiorstwa wykonawcy: Średni przedsiębiorca

7.3.) Dane (firmy) wykonawcy, któremu udzielono zamówienia:

7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia: ANZENA Sp. z o.o.

7.3.2) Krajowy Numer Identyfikacyjny: 9542739396

7.3.4) Miejscowość: Katowice

7.3.6.) Województwo: śląskie

7.3.7.) Kraj: Polska

7.3.8.) Czy wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcom?: Nie

SEKCJA VIII UMOWA (dla części 3)

8.1.) Data zawarcia umowy: 2022-12-14

8.2.) Wartość umowy/umowy ramowej: 6124,17 PLN

8.3.) Okres realizacji zamówienia albo umowy ramowej: 14 dni