Ogłoszenie o wyniku postępowania
Usługi
„Zakup macierzy” w ramach zadania: „zakupy inwestycyjne – w ramach realizacji programu pn. „Cyberbezpieczny Samorząd”
w ramach Funduszu Europejskiego na Rozwój Cyfrowy 2021-2027 (FERC)

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego
Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: Gmina Kaliska

1.4) Krajowy Numer Identyfikacyjny: REGON 191675698

1.5) Adres zamawiającego

1.5.1.) Ulica: Nowowiejska 2

1.5.2.) Miejscowość: Kaliska

1.5.3.) Kod pocztowy: 83-260

1.5.4.) Województwo: pomorskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL638 - Starogardzki

1.5.7.) Numer telefonu: 585889201

1.5.8.) Numer faksu: 585889206

1.5.9.) Adres poczty elektronicznej: sekretariat@kaliska.pl

1.5.10.) Adres strony internetowej zamawiającego: www.kaliska.pl

1.6.) Adres strony internetowej prowadzonego postępowania:
https://platformazakupowa.pl/pn/kaliska/proceedings

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 macierzy” w ramach zadania: „zakupy inwestycyjne – w ramach realizacji programu pn. „Cyberbezpieczny Samorząd”
w ramach Funduszu Europejskiego na Rozwój Cyfrowy 2021-2027 (FERC)

2.4.) Identyfikator postępowania: ocds-148610-44c38571-b58f-44ba-993c-6e9fdbdd6587

2.5.) Numer ogłoszenia: 2024/BZP 00605418

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2024-11-20

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

2.9.) Numer planu postępowań w BZP: 2024/BZP 00012930/06/P

2.10.) Identyfikator pozycji planu postępowań:

1.3.3 „Zakup macierzy” w ramach zadania: „zakupy inwestycyjne – w ramach realizacji programu pn. „Cyberbezpieczny Samorząd” w ramach Funduszu Europejskiego na Rozwój Cyfrowy 2021-2027 (FERC)

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

2.12.) Nazwa projektu lub programu:
Program „Cyberbezpieczny Samorząd" w ramach Funduszu Europejskiego na Rozwój Cyfrowy 2021-2027 (FERC)

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

2.14.) Numer ogłoszenia: 2024/BZP 00561061

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: ZP.271.26.2024

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

4.4.) Rodzaj zamówienia: Usługi

4.5.1.) Krótki opis przedmiotu zamówienia

Zadanie obejmuje:
1.
dostawę i wdrożenie dedykowanej macierzy do backupu wraz z oprogramowaniem w siedzibie Urzędu Gminy w Kaliskach (Nowowiejska 2, 83-260 Kaliska)
2.
wykonanie odmiejscowienia backupu Urzędu Gminy w Kaliskach i wyniesienie do lokalizacji budynek Ochotniczej Straży Pożarnej w Kaliskach (ul. Nowowiejska 2b)
3.
usługi przedwdrożeniowe i wdrożenie,
i traktowane jest jako całość.
1.
Zamawiający wymaga dostarczenia i wdrożenia macierzy do backupu z dedykowanym oprogramowaniem oraz infrastrukturą sieciową, niezbędną do wykonania odmiejscowienia backupu na urządzeniu klasy NAS będącego własnością Zamawiającego (QNAP TS-431x).
a) Wymagania minimalne dla macierzy do backupu z dedykowanym oprogramowaniem (dostawa i wdrożenie obejmują 1 komplet):
1.
Zarządzanie i magazyny
1.
Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024r.
2.
System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3.
Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
a.
Obudowa Rack 1U,
b.
Procesor: min. 6 rdzeni, min. 12 wątków. Minimalna częstotliwość bazowa procesora 2.9GHz,
c.
Pamięć RAM: min. 16GB DDR4,
d.
Przestrzeń dostępna na przechowywanie danych: min. 24 TB po RAID 5,
e.
Osobne dyski SSD M.2 NVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,
f.
Redundantne zasilanie,
g.
Interfejsy sieciowe: min. 2 szt. Ethernet 1Gb,
h.
Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania.
4.
Produkt dostępny w polskiej wersji językowej.

5.
Konsola zarządzająca dostępna z poziomu przeglądarki internetowej.
6.
System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków.
7.
System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów.
8.
System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych.
9.
System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT.
10.
System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft.
11.
Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe.
12.
System zarządzania nie może być oparty o relacyjne bazy danych.
13.
Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
14.
Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
15.
Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
16.
Rozwiązanie musi być systemem multi-storage i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
17.
System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
18.
System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
19.
System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
20.
Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
21.
Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
22.
System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
23.
Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych.
24.
Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
25.
System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
26.
System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
27.
Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
28.
Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
29.
System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane

przez użytkownika.
30.
Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
31.
Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
32.
Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
33.
System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
34.
Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
35.
Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych.
36.
Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
37.
Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
38.
Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
39.
Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
40.
Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
41.
System musi pozwalać na automatyczne aktualizacje oprogramowania.
42.
System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
43.
System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
44.System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
45.System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
46.Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
47.System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
48.System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
49.Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
50.W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.

Pełen opis przedmiotu zamówienia znajduje się w zał. nr 9 - OPZ

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

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA

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

SEKCJA VI OFERTY

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: 200490 PLN

6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 200490 PLN

6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 200490 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

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

7.2.) Wielkość przedsiębiorstwa wykonawcy: Mikro przedsiębiorca

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

7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia: Login IT Jacek Zimny

7.3.2) Krajowy Numer Identyfikacyjny: 5921474043

7.3.3) Ulica: Zięby 5

7.3.4) Miejscowość: Koteże

7.3.5) Kod pocztowy: 83-200

7.3.6.) Województwo: pomorskie

7.3.7.) Kraj: Polska

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

SEKCJA VIII UMOWA

8.1.) Data zawarcia umowy: 2024-11-19

8.2.) Wartość umowy/umowy ramowej: 200490 PLN

8.3.) Okres realizacji zamówienia albo umowy ramowej: 30 dni