Załącznik nr 1 do Ogłoszenia o zamówieniu

Opis przedmiotu zamówienia

Według oznaczenia Wspólnego Słownika Zamówień (CPV):
72317000-0 – usługi przechowywania danych
72319000-4 – usługi dostarczania danych
72318000-7 – usługi przesyłu danych

1. Przedmiotem zamówienia jest świadczenie usługi przechowywania i udostępniania plików w chmurze (Object Storage) **przez okres 24 miesięcy od dnia 01.03.2025 r. lub do wyczerpania kwoty, którą Zamawiający przeznaczył na realizację zamówienia w wysokości 70 000,00 zł brutto**, o poniższych wymaganiach:
   1.1. Pliki przesłane do storage muszą być dostępne publicznie pod stałym adresem url.;
   1.2. Storage space (GB): min. 3000;
   1.3. Transfer (TB/mc): min. 40;
   1.4. Interfejs do wymiany danych: Openstack-swift albo kompatybilny z S3;
   1.5. Dostępność: min. 99,9%
      a) dobowo: max. 1m 26.4s
      b) tygodniowo: max. 10m 4.8s
      c) miesięcznie: max. 43m 49.7s
   1.6. Dostępne rozszerzenie typu rsync lub inne stosowane w tworzeniu narastających kopii zapasowych.
   1.7. Zgodność technologiczna chmury (Object Storage) z polityką **CORS** (ang. *Cross-Origin Resource Sharing)* tj. usługa powinna mieć możliwość konfigurowania polityki CORS poprzez ustawienie odpowiednich nagłówków w odpowiedzi http.
   1.8. Lokalizacja infrastruktury chmurowej na terenie UE.
2. **Wykonawca zapewni usługę opieki technicznej i serwisowej obejmującą:**
   2.1. reagowanie na zgłoszenia serwisowe Zamawiającego w przypadku wykrycia nieprawidłowości w funkcjonowaniu usługi;
   2.2. zapewnienie działania ciągłości świadczonej usługi 24/7/365 dni.
   2.3. świadczenie usługi na zasadach SLA o wymaganej niezawodności w okresie rozliczeniowym na poziomie: 99,9%.

3. **Czasy reakcji:**

   Wykonawca zapewni wsparcie techniczne w dni robocze od godz. 8:00 do godz. 16:00, z uwzględnieniem następujących czasów reakcji na zgłoszenie:
   a) 4 godziny diagnostyka problemu, 48 godzin wymiana lub naprawa wadliwego sprzętu w przypadku otrzymania zgłoszenia w godzinach pracy (dni robocze, od godz. 8:00 do godz. 16:00);
   b) 4 godziny diagnostyka problemu, 48 godzin wymiana lub naprawa wadliwego sprzętu licząc od godziny 8:00 w najbliższym dniu roboczym w przypadku otrzymania zgłoszenia poza godzinami pracy.

4. Bezpieczeństwo.

4.1. Bezpieczeństwo informatyczne

1. Usługi przechowywania i udostępniania plików w chmurze w obszarze realizacji zasad bezpieczeństwa musi spełniać wymagania techniczne i organizacyjne wynikające z regulacji określonych normą PN/ISO 27001 lub równoważną oraz z norm wynikających z przepisów prawa, w szczególności rozporządzenia Rady Ministrów z dnia 21 maja 2024r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, 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), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a także aktualnie obowiązujących w tym zakresie regulacji prawnych, zmieniających lub zastępujących wskazane akty prawne. Usługi przechowywania i udostępniania plików w chmurze powinny zapewniać ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, w szczególności przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) usługi przechowywania i udostępniania plików w chmurze muszą być kompatybilne z analizatorami logów, w szczególności wymagana jest możliwość pełnego logowania do systemu zewnętrznego,
   d) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,
   e) dbałość o aktualizację oprogramowania,
   f) minimalizowanie ryzyka utraty informacji w wyniku awarii,
   g) ochronę przed błędami, utratą, nieuprawnioną modyfikacją,
   h) zgłaszanie Zamawiającemu incydentów mających wpływ na bezpieczeństwo przetwarzanych informacji,
   i) niezwłoczne podejmowanie działań po dostrzeżeniu podatności mających wpływ na możliwość naruszenia bezpieczeństwa informacji.
2. W tym celu wymagane jest stosowanie następujących mechanizmów:
   a) ochrona i kontrola dostępu (zapora UTM - skrót od ang. Unified Threat Management) na styku z Internetem – odrzucanie niepożądanego ruchu sieciowego,
   b) separacja ruchu kierowanego do urządzeń na których przechowywane są dane klienta, Zamawiający nie oczekuje konkretnego mechanizmu separacji.
   c) system wykrywania i zapobiegania włamaniom (IDS/IPS – skrót od ang. Intrusion Detection System/ Intrusion Prevention System).
3. Ze względu na wrażliwość danych wymagane jest:

a) w przypadku awarii dysków w serwerach lub macierzach, przesłanie wymienionych dysków do Zamawiającego,
b) po zakończeniu okresu funkcjonowania Usługi, dane znajdujące się na macierzach dyskowych muszą zostać trwale usunięte przez Wykonawcę w obecności przedstawiciela Zamawiającego, co musi zostać potwierdzane protokołem zniszczenia danych podpisanym przez Wykonawcę i Zamawiającego.

4.2. Kontrola dostępu i ochrona fizyczna.

Miejsce przechowywania danych musi posiadać wielostopniowy system ochrony fizycznej i kontroli dostępu. W szczególności oznacza to:

- całodobową ochronę przez kwalifikowanych pracowników ochrony wejść do budynku i terenu wokół niego;
- monitoring obiektu przy pomocy kamer telewizji przemysłowej CCTV;
- zabezpieczenie obiektu przy pomocy systemu alarmowego.

5. MONITORING I ZARZĄDZANIE

5.1. Monitoring infrastruktury.

Świadczący usługę musi zapewniać monitoring infrastruktury dla usługi przechowywania i udostępniania plików klienta (klasy The Ultimate Enterprise-class Monitoring Platform, np. Zabbix lub równoważne) Niedostępność usług musi być raportowana do klienta przy pomocy e-maili oraz komunikatu SMS; dodatkowo mogą być stosowane inne mechanizmy powiadomień np. push notification. Zamawiający musi posiadać dostęp do systemu monitoringu w trybie minimum do odczytu. Zamawiający musi posiadać możliwość prowadzenia monitoringu we własnych systemach, tj. Zabbix. Wykonawca odpowiada za monitoring niezależnie od monitoringu prowadzonego przez Zamawiającego.

5.2. Statystyki ruchu.

Zamawiający musi mieć dostęp do statystyk ruchu wejściowego i wyjściowego ze swojej infrastruktury. Dostęp musi być całodobowy i odbywać się za pomocą strony internetowej. Zamawiający również musi posiadać możliwość prowadzenia tych statystyk we własnych systemach monitoringu, tj. Zabbix.