OPIS PRZEDMIOTU ZAMÓWIENIA

Opis przedmiot zamówienia dla części I i II

1. Nazwa zamówienia

Świadczenie usługi dostępu do Internetu oraz usługi antyDDos (zwane dalej „**Usługi**") przez okres 12 miesięcy (2 części).

2. Przedmiot zamówienia

Część I -Świadczenie usługi dostępu do Internetu oraz usługi antyDDos w lokalizacji I (Warszawa, ul. Olszewska 6) od dnia 03.08.2022 do dnia 03.08.2023 r.

Część II -Świadczenie usługi dostępu do Internetu oraz usługi antyDDos w lokalizacji II (Warszawa, ul. Pawińskiego 17/21) od dnia 28.07.2022 do dnia 28.07.2023 r.

3. Kody CPV 72411000-4 - Dostawcy usług internetowych (ISP).

4. Wymagania ogólne dla realizacji przedmiotu zamówienia dla Części I i Części II:

1. Wykonawca w ramach realizacji zamówienia dostarczy, zainstaluje i skonfiguruje sprzęt niezbędny do prawidłowego świadczenia Usług oraz utrzyma go w stanie zapewniającym świadczenie Usługi zgodnie z parametrami określonymi poniżej.
2. Zamawiający dopuszcza instalację przez Wykonawcę, w siedzibie Zamawiającego i w Lokalizacji odpowiednio I lub II, niezbędnych do aktywacji i świadczenia usług telekomunikacyjnych urządzeń, na koszt i ryzyko Wykonawcy, o ile będzie to konieczne do prawidłowej realizacji przedmiotu zamówienia. Przez Lokalizacje rozumie się wskazane przez Zamawiającego dwie lokalizacje (Lokalizacja I i Lokalizacja II) znajdujące się na terenie m.st. Warszawy wskazane w pkt 2 OPZ, w których ma nastąpić aktywacja;
3. Zamawiający udostępni Wykonawcy w szafie serwerowej w Lokalizacji odpowiednio I lub II miejsce o wysokości 1U wraz z zasilaniem 230V.
4. Usługi dostępu do Internetu będą świadczone 24/7/365, począwszy:
    a. w części I od dnia 03.08.2022 do 03.08.2023 r.
    b. w części II od dnia 28.07.2022 do 28.07.2023 r.

    z zachowaniem wszystkich parametrów określonych poniżej. Do dni wskazanych powyżej dla każdej z Lokalizacji, Wykonawca przeprowadzi wszystkie niezbędne czynności w zakresie przyłączenia łącza internetowego tak, aby zapewnić bezprzerwową zmianę operatora, w tym przeprowadzi wraz z Zamawiającym testy sprawności Usługi.
5. Jeden Wykonawca może podpisać umowę wyłącznie na świadczenie Usługi w jednej z dwóch Części (Lokalizacji I albo Lokalizacji II).

5. Szczegółowe warunki świadczenia Usług dla Części I i Części II:

1. Parametry łącza dla Lokalizacji I (ul. Olszewska 6, Warszawa)
   1) typ łącza: symetryczne;
   2) gwarantowana przepustowość 10 Gb/s;
   3) łącze zakończone w technologii TenGigabit Ethernet stykiem XFP LC/LC (TX/RX oddzielne tory);
   4) musi posiadać pełne pasma do routera brzegowego Wykonawcy;
   5) musi obsługiwać protokół BGP (zewnętrzny protokół trasowania) w pełnej funkcjonalności;
   6) opóźnienia w ramach sieci nie mogą być większe niż 20ms do routera brzegowego;
   7) łącze nie może posiadać ograniczeń transferu oraz nie może posiadać zablokowanych portów;
   8) Wykonawca dostarczy wkładkę do routera Cisco XFP-10GLR-OC192SR oraz 30 metrowy patchcord single mode duplex.
2. Parametry łącza dla Lokalizacji II (ul. Pawińskiego 17/21, Warszawa):
   1) typ łącza: symetryczne;
   2) gwarantowana przepustowość 10 Gb/s;
   3) łącze zakończone w technologii Tengigabit Ethernet stykiem XFP LC/LC (TX/RX oddzielne tory);
   4) musi posiadać pełne pasma do routera brzegowego Wykonawcy;
   5) musi obsługiwać protokół BGP (zewnętrzny protokół trasowania)w pełnej funkcjonalności;
   6) opóźnienia w ramach sieci nie mogą być większe niż 20ms do routera brzegowego;
   7) łącze nie może posiadać ograniczeń transferu oraz nie może posiadać zablokowanych portów.

6. Pozostałe wymagania świadczenia Usług dla Części I i Części II :

1) Wykonawcy w ramach przedmiotu Umowy są zobowiązani rozgłaszać sieć Zamawiającego 185.41.93.0/24 oraz 2A01:53A0:1::/48 AS199953 protokołem BGP (zewnętrzny protokół trasowania).
2) Łącza nie mogą być zrealizowane w technologii radiowej. Łącza muszą być zrealizowane w technologii światłowodowej.
3) Zapewniona zostanie ochrona przeciw atakom DDoS oraz Do S, realizowana sprzętowo na poziomie sieci operatora (blackholing). Ochrona musi zapewniać również ochronę przed atakami typu flood, sweep, teardrop oraz smurf dla min. protokołów HTTP/HTTPS, SIP, DNS.
4) Wykonawca jest zobowiązany do niezwłocznego przekazania Zamawiającemu każdorazowo alertu o rozpoczęciu oraz o zakończeniu próby ataku poprzez wiadomość sms oraz na adres e-mail Zamawiającego.
5) Zamawiającemu zostanie zapewniony dostęp za pośrednictwem sieci Internet do systemu antyDDoS w celu monitorowania, podglądu oraz analizy incydentów w dniach aktywacji dla obu Lokalizacji. Dostęp do systemu antyDDoS będzie możliwy ze wskazanych przez Zamawiającego publicznych adresów IP oraz nie może wiązać się z koniecznością zestawiania dodatkowych tuneli VPN, oraz dodatkowych mechanizmów uwierzytelniania użytkowników opartych o tokeny.
6) Zamawiającemu zostanie zapewniony dostęp poprzez jednoczesne logowanie się minimum 10 użytkowników do systemu antyDDoS.

7) Awarie będą zgłaszane w trybie 24/7/365, poprzez email, telefon lub elektroniczny system zgłoszeniowy. Przez Awarię rozumie się stan, w którym nie jest możliwe korzystanie z Usług w sposób zgodny z OPZ lub celem Umowy lub inne nieprawidłowe działanie Usług. Zgłoszenie - poinformowanie Wykonawcy przez Zamawiającego o wystąpieniu Awarii. Za chwile dokonania Zgłoszenia Awarii Zamawiający uznaje datę i godzinę jego zgłoszenia przez jeden z kanałów, o których mowa w tym punkcie. W przypadku zgłoszenia Awarii przez więcej niż jeden kanał, chwilą dokonania Zgłoszenia będzie wcześniejsza data i godzina.
8) Czas reakcji (czas liczony od zgłoszenia do momentu potwierdzenia jego otrzymania przez Wykonawcę) wynosi maksymalnie do 1 godziny od Zgłoszenia. Za moment potwierdzenia otrzymania zgłoszenia przez Wykonawcę, uznaje się moment otrzymania przez Zamawiającego wiadomości e-mail.
9) W przypadku gdy Wykonawca wykryje Awarię jest zobowiązany do niezwłocznego poinformowania Zamawiającego o jej wystąpieniu poprzez wysłanie wiadomości email.
10) Usunięcie Awarii łącza w terminie maksymalnie do 24 godzin od jej Zgłoszenia (stanowi dodatkowe kryterium oceny ofert) lub od chwili poinformowania Zamawiającego przez Wykonawcę o Awarii, zgodnie z pkt 8) powyżej.
11) Dostępność łącza w skali miesiąca to co najmniej 99%.
12) Wykonawca oświadcza, że jest świadomy, iż z uwagi na wymogi bezpieczeństwa, obowiązujące w Lokalizacji I oraz Lokalizacji II, osoby wyznaczone przez Wykonawcę do realizacji prac mogą być zobowiązane do okazania służbom ochrony obiektów, przed rozpoczęciem świadczenia prac w danej Lokalizacji, aktualnego zaświadczenia o niekaralności (informacja z Krajowego Rejestru Karnego).
13) Realizacja przedmiotu zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt 7 Ustawy o Krajowym systemie cyberbezpieczeństwa, dalej: „Ustawa", należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, przedmiot zamówienia musi być zgodny z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

7. Pozostałe zasady realizacji niniejszego zamówienia określone zostały w Rozdziale III SWZ – Projektowane Postanowienia Umowy.