

Opis przedmiotu zamówienia dla części I i II

Świadczenie usługi dostępu do sieci Internet i usługi antyDDoS przez okres 36 miesięcy.

1. Oznaczenie przedmiotu zamówienia wg Kod CPV:

72411000-4 - Dostawcy usług internetowych (ISP).

2. Definicje:

Na potrzeby niniejszego dokumentu, określenia poniższe będą miały następujące znaczenie:

1. **Awaria** – stan, w którym nie jest możliwe korzystanie z Usług w sposób zgodny z OPZ lub celem Umowy lub inne nieprawidłowe działanie Usług;
2. **Aktywacja** – moment uruchomienia Usługi w danej Lokalizacji, potwierdzony protokołem odbioru;
3. **Dni robocze** – dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej;
4. **Lokalizacje** – wskazane przez Zamawiającego dwie lokalizacje (Lokalizacja I i Lokalizacja II) znajdujące się na terenie m.st. Warszawy wskazane w pkt 4 OPZ, w których ma nastąpić Aktywacja;
5. **Usługi** – usługa dostępu do Internetu wraz z usługą antyDDoS świadczona przez okres 36 miesięcy od dnia Aktywacji.
6. **Zgłoszenie** - poinformowanie Wykonawcy przez Zamawiającego o wystąpieniu Awarii. Za chwilę dokonania Zgłoszenia Awarii Zamawiający uznaje datę i godzinę jego zgłoszenia przez jeden z kanałów, o których mowa w pkt 7.2.7 OPZ. W przypadku zgłoszenia Awarii przez więcej niż jeden kanał, chwilą dokonania Zgłoszenia będzie wcześniejsza data i godzina.
7. **Czas Obsługi** - czas usunięcia Awarii, okres od dokonania Zgłoszenia do momentu, w jakim zostanie przywrócone prawidłowe świadczenie Usługi.

3. Przedmiot zamówienia:

Część I - Świadczenie usługi dostępu do Internetu wraz z usługą antyDDoS w Lokalizacji I (Warszawa, Pawińskiego 17/21) przez okres 36 miesięcy.

Część II - Świadczenie usługi dostępu do Internetu wraz z usługą antyDDoS w Lokalizacji II (Warszawa, ul. 11 Listopada 23) przez okres 36 miesięcy.

4. Termin realizacji Aktywacji przedmiotu zamówienia:

Aktywacja musi nastąpić maksymalnie w ciągu 21 Dni roboczych¹ od dnia zawarcia Umowy.

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

1. Wykonawca w ramach realizacji zamówienia uruchomi Usługi oraz zapewni ich świadczenie zgodnie z parametrami określonymi w pkt. 7 OPZ przez okres 36 miesięcy od dnia Aktywacji.

¹ Stanowi dodatkowe kryterium oceny Ofert.

2. Zamawiający dopuszcza instalację przez Wykonawcę, odpowiednio w Lokalizacji I lub Lokalizacji II, niezbędnych do Aktywacji i świadczenia Usług urządzeń, o ile będzie to niezbędne do prawidłowej realizacji przedmiotu zamówienia, na koszt i ryzyko Wykonawcy.
3. Zamawiający udostępni Wykonawcy, odpowiednio w Lokalizacji I lub Lokalizacji II, w szafie serwerowej miejsce o wysokości 1U wraz z zasilaniem 230V.
4. Usługi będą świadczone 24/7/365.
5. **Jeden Wykonawca może podpisać umowę wyłącznie na świadczenie Usługi w jednej z dwóch Części (Lokalizacji I albo Lokalizacji II).**

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

Parametry łącza dla każdej z dwóch Lokalizacji:

1. Typ łącza: symetryczne;
2. Gwarantowana przepustowość 1 Gb/s;
3. Łącze zakończone w technologii Gigabit Ethernet stykiem RJ-45
4. Musi posiadać pełne pasma do routera brzegowego Wykonawcy;
5. Musi obsługiwać protokół BGP (Border Gateway Protocol) w pełnej funkcjonalności;
6. Opóźnienia w ramach sieci nie mogą być większe niż 20ms do routera brzegowego Wykonawcy;
7. Łącze nie może posiadać ograniczeń transferu oraz nie może posiadać zablokowanych portów.
8. Wykonawca w ramach przedmiotu zamówienia jest zobowiązany rozgłaszać sieć Zamawiającego IPv4 i IPv6 protokołem BGP (Border Gateway Protocol);
9. Łącza muszą być zrealizowane w technologii światłowodowej;
10. Zapewniona zostanie ochrona przeciw atakom DDoS oraz DoS realizowana sprzętowo na poziomie sieci operatora (blackholing). Ochrona musi zapewniać również ochronę przed atakami typu flood, Sweep, teardrop oraz smurf dla między innymi: protokołów HTTP/HTTPS, SIP, DNS;
11. 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;
12. Wykonawca nie później niż 8 godzin po zakończeniu próby ataku przekaże Zamawiającemu listę 100 najaktywniejszych IP;
13. Jeden raz w miesiącu, nie później niż do 3 Dnia roboczego kolejnego miesiąca, Wykonawca przekaże Zamawiającemu raport za poprzedni miesiąc, który będzie zawierał zestawienia (wykres typu Stacked):
 - bps;
 - ppsoraz zestawienie alertów zawierające:
 - Maximum Severity Percent;
 - Maximum Impact Of Alert Traffic bps;
 - Maximum Impact Of Alert Traffic pps.
14. Zamawiający wskaże w Umowie numery telefonów oraz adresy e-mail, na które Wykonawca będzie przekazywał alerty i raporty o których mowa w pkt. 11. – 13.;
15. Zamawiającemu zostanie zapewniony dostęp za pośrednictwem sieci Internet do systemu antyDDoS w celu monitorowania, podglądu oraz analizy incydentów. Dostęp do systemu antyDDoS będzie możliwy ze wskazanych w Umowie przez Zamawiającego publicznych adresów IP oraz nie może wiązać się z koniecznością zestawiania dodatkowych tuneli VPN, oraz dodatkowych mechanizmów uwierzytelniania użytkowników opartych o tokeny;

16. Zamawiającemu zostanie zapewniony dostęp poprzez jednoczesne logowanie się minimum 20 użytkowników do systemu antyDDoS;
 17. Awarie będą zgłaszane przez Zamawiającego w trybie 24/7/365 poprzez e-mail i telefon;
 18. 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;
 19. W przypadku gdy Wykonawca wykryje Awarię jest zobowiązany do niezwłocznego poinformowania Zamawiającego o jej wystąpieniu poprzez wysłanie wiadomości e-mail;
 20. **Czas Obsługi wynosi maksymalnie do 24 godzin od Zgłoszenia lub od chwili poinformowania Zamawiającego przez Wykonawcę o Awarii, zgodnie z pkt 12.²;**
 21. Gwarantowana przez Wykonawcę dostępność Usług w skali miesiąca to co najmniej 99%.
2. Wykonawca oświadcza, że jest świadomy, iż z uwagi na wymogi bezpieczeństwa, obowiązujące w Lokalizacjach, 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).
 3. 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 (tj. Dz. U z 2020 r. poz. 1369), 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.
 4. Pozostałe zasady realizacji niniejszego zamówienia określone zostały w Rozdziale III SWZ – Projektowane Postanowienia Umowy

² Stanowi dodatkowe kryterium oceny Ofert.