

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Nazwa zamówienia

Świadczenie usługi dostępu do sieci Internet i usługi antyDDoS w dwóch lokalizacjach przez okres 12 miesięcy (2 części).

2. Oznaczenie przedmiotu zamówienia wg CPV

72411000-4 - Dostawcy usług internetowych (ISP).

3. Definicje

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

Awaria	Stan, w którym nie jest możliwe korzystanie z Usług w sposób zgodny z OPZ lub inne nieprawidłowe działanie Usług.
Aktywacja	Moment uruchomienia Usługi w danej Lokalizacji, potwierdzony protokołem odbioru.
Dni robocze	Dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.
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.
Usługi	Usługa dostępu do Internetu wraz z usługą antyDDoS świadczona przez okres 12 miesięcy od dnia Aktywacji.
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.
Czas Obsługi	Czas usunięcia Awarii, okres od dokonania Zgłoszenia do momentu, w jakim zostanie przywrócone prawidłowe świadczenie Usługi.

4. Określenie przedmiotu zamówienia

Przedmiotem zamówienia jest:

- 4.1 Część I/Wariant 1 - Świadczenie usługi dostępu do Internetu w Lokalizacji I (znajdująca się na terenie m.st. Warszawy) przez okres 12 miesięcy od dnia 26 września 2026 r.
- 4.2 Część I/Wariant 2 - Świadczenie usługi dostępu do Internetu wraz z **usługą antyDDoS** w Lokalizacji I (znajdująca się na terenie m.st. Warszawy) przez okres 12 miesięcy od dnia 26 września 2026 r.
- 4.3 Część II/Wariant 1 - Świadczenie usługi dostępu do Internetu w Lokalizacji II (znajdująca się na terenie m.st. Warszawy) przez okres 12 miesięcy od dnia 21 października 2026 r.
- 4.4 Część II/Wariant 2 - Świadczenie usługi dostępu do Internetu wraz z **usługą antyDDoS** w Lokalizacji II (znajdująca się na terenie m.st. Warszawy) przez okres 12 miesięcy od dnia 21 października 2026 r.

5. Termin realizacji – aktywacja przedmiotu zamówienia

5.1 Aktywacja musi nastąpić:

- Dla części I – najpóźniej od dnia 26 września 2026 r.;
- Dla części II – najpóźniej od dnia 21 października 2026 r.

6. Wymagania ogólne dla realizacji przedmiotu zamówienia w Lokalizacji I i Lokalizacji II:

- 6.1 Wykonawca w ramach realizacji zamówienia uruchomi Usługi oraz zapewni ich świadczenie zgodnie z parametrami określonymi w pkt. 7 OPZ przez okres 12 miesięcy od dnia Aktywacji.
- 6.2 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.
- 6.3 Zamawiający udostępni Wykonawcy, odpowiednio w Lokalizacji I lub Lokalizacji II, w szafie serwerowej miejsce o wysokości 1U wraz z zasilaniem 230V.
- 6.4 Usługi będą świadczone 24/7/365.
- 6.5 Jeden Wykonawca może podpisać umowę wyłącznie na świadczenie Usługi w jednej z dwóch Lokalizacji (Lokalizacji I albo Lokalizacji II).

7. Szczegółowe warunki świadczenia Usług w Lokalizacji I i Lokalizacji II

- 7.1 Parametry łącza dla każdej z dwóch Lokalizacji:
 - 7.1.1 Typ łącza: symetryczne;
 - 7.1.2 Gwarantowana przepustowość 10 Gb/s; opcjonalnie przepustowość 100 GB/s
 - 7.1.3 Łącze zakończone w technologii TenGigabit Ethernet stykiem SFP+ LC/LC (TX/RX oddzielne tory). W sposób kompatybilny z modułem - 10GBASE-SR/LR, opcjonalnie 100GBASE-SR/LR. Zamawiający zastrzega sobie możliwość zmiany typu zakończenia łącza w porozumieniu z Wykonawcą;
 - 7.1.4 Musi posiadać pełne pasma do routera brzegowego Wykonawcy;
 - 7.1.5 Musi obsługiwać protokół BGP (Border Gateway Protocol) w pełnej funkcjonalności;
 - 7.1.6 Opóźnienia w ramach sieci nie mogą być większe niż 20ms do routera brzegowego Wykonawcy;
 - 7.1.7 Łącze nie może posiadać ograniczeń transferu oraz nie może posiadać zablokowanych portów.
- 7.2 Pozostałe wymagania świadczenia Usług w Lokalizacji I i Lokalizacji II:
 - 7.2.1 Wykonawca w ramach przedmiotu zamówienia jest zobowiązany rozgłaszać sieć Zamawiającego IPv4 i IPv6 protokołem BGP (Border Gateway Protocol). W ramach protokołu BGP będzie możliwość uruchomienia mechanizmu szybkiego wykrywania awarii opartego na BFD (RFC 5880) w interwale czasowym mniejszym niż 1 sekunda. (optymalnie 3x300ms).
 - 7.2.2 Łącza muszą być zrealizowane w technologii światłowodowej;
 - 7.2.3 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;
 - 7.2.4 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;
 - 7.2.5 Wykonawca nie później niż 8 godzin po zakończeniu próby ataku przekaże Zamawiającemu listę 100 najaktywniejszych IP;

- 7.2.6 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;
 - pps;
- oraz zestawienie alertów zawierające:
- Maximum Severity Percent;
 - Maximum Impact Of Alert Traffic bps;
 - Maximum Impact Of Alert Traffic pps.
- 7.2.7 Zamawiający wskaże w Umowie numery telefonów oraz adresy e-mail, na które Wykonawca będzie przekazywał alerty i raporty o których mowa w pkt. 7.2.4 – 7.2.6;
- 7.2.8 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;
- 7.2.9 Zamawiającemu zostanie zapewniony dostęp poprzez jednoczesne logowanie się minimum 20 użytkowników do systemu antyDDoS;
- 7.2.10 Awarie będą zgłaszane przez Zamawiającego w trybie 24/7/365 poprzez e-mail i telefon;
- 7.2.11 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;
- 7.2.12 W przypadku, gdy Wykonawca wykryje Awarię jest zobowiązany do niezwłocznego poinformowania Zamawiającego o jej wystąpieniu poprzez wysłanie wiadomości e-mail;
- 7.2.13 Czas Obsługi wynosi maksymalnie do 4 godzin od Zgłoszenia lub od chwili poinformowania Zamawiającego przez Wykonawcę o Awarii, zgodnie z pkt 7.2.12 .;
- 7.2.14 Gwarantowana przez Wykonawcę dostępność Usług w skali miesiąca to co najmniej 99%.
- 7.2.15 Wykonawca jest świadomy, że ze względu na wymogi bezpieczeństwa obowiązujące w Lokalizacjach, osoby wyznaczone przez Wykonawcę do realizacji przedmiotu Umowy mogą być zobowiązane do okazania służbom ochrony obiektów, przed wykonaniem dostawy lub rozpoczęciem świadczenia prac, usług w danej Lokalizacji poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli co najmniej „POUFNE” lub innego dokumentu np. aktualnego zaświadczenia o niekaralności (informacja z Krajowego Rejestru Karnego). W przypadku odmowy wstępu do Lokalizacji przez służby ochrony obiektu z powodu nieokazania przez daną osobę ww. dokumentów, opóźnienie w realizacji przedmiotu Umowy z tego wynikające będzie stanowiło zwłokę Wykonawcy.
- 7.2.16 Realizacja przedmiotu zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z **art. 5 ust 1 pkt 4 lit. d w zw. z art. 4 pkt. 1 Ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026. poz. 20 ze zm.)**, 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, Oprogramowanie musi być zgodne z **obowiązującymi przepisami prawa w zakresie cyberbezpieczeństwa, w tym z Ustawą o krajowym systemie cyberbezpieczeństwa, oraz że jego wykorzystanie nie będzie powodować powstania nieuzasadnionych zagrożeń dla cyberbezpieczeństwa, bezpieczeństwa publicznego ani istotnych interesów bezpieczeństwa państwa.**

- 7.3 Zamawiający przekaze adresy lokalizacji (Część I i Część II) Wykonawcom, którzy złożą do Zamawiającego wniosek o udostępnienie takich informacji, zgodnie z procedurą, obejmującą między innymi: złożenie wniosku w formie elektronicznej, wg wzoru przygotowanego przez Zamawiającego, złożenie umowy o zachowaniu poufności wg wzoru przygotowanego przez Zamawiającego, udostępnienie przez Zamawiającego informacji poprzez wysłanie zaszyfrowanego dokumentu za pośrednictwem poczty elektronicznej oraz hasła za pośrednictwem wiadomości SMS.