Załącznik nr 1 do umowy nr …….

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest świadczenie usługi dostępu do Internetu oraz usługi monitorowania bezpieczeństwa i aktywnej ochrony przed atakami sieciowymi oraz atakami DDoS przez okres 36 miesięcy dla Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego.

Umowa obejmować będzie przyłącza w następujących lokalizacjach Urzędu Marszałkowskiego:

1) Toruń, ul. Plac Teatralny 2
2) Toruń, ul. Św. Jana 1/3
3) Toruń, ul. Targowa 13-15
4) Toruń, ul. M. Skłodowskiej-Curie 73
5) Toruń, ul. Kopernika 4
6) Toruń, Arpol
7) Bydgoszcz, ul. Jagiellońska 9
8) Bydgoszcz, ul. Gimnazjalna 2a
9) Włocławek, ul. Bechiego 2
10) Grudziądz, ul. Waryńskiego 4
11) Toruń, ul. Franciszkańska 12

Dokładne wyznaczenie miejsc dla punktów przyłącza określi Zamawiający, po uzgodnieniu z Wykonawcą w ramach przeprowadzonej wizji lokalnej.

1. **Wymagania ogólne dla realizacji przedmiotu zamówienia:**

1) Umowa na świadczenie usługi dostępu do Internetu zostanie podpisana na okres 36 miesięcy.
2) Wykonawca w ramach realizacji zamówienia dostarczy, zainstaluje i skonfiguruje sprzęt niezbędny do prawidłowego świadczenia Usług oraz utrzyma go w stanie zapewniającym świadczenie Usług zgodnie z parametrami określonymi poniżej.
3) Ewentualne koszty instalacji i aktywacji usługi dostępu do Internetu powinny być wliczone do kosztów miesięcznych abonamentów, zawartych w formularzu cenowym.
4) Wykonawca dostarczy i zainstaluje urządzenia dostępowe – routery/modemy do udostępniania połączenia internetowego.
5) Urządzenia dostępowe pozostają własnością Wykonawcy i powinny być przez niego i na jego koszt serwisowane oraz ubezpieczone od kradzieży lub zniszczenia.
6) Zamawiający udostępni Wykonawcy miejsce w szafie serwerowej wraz z zasilaniem 230V.
7) Zamawiający umożliwi Wykonawcy dostęp do lokalizacji, celem aktywacji Usług, a następnie ich świadczenia.

2. Specyfikacja techniczna połączeń internetowych.

	Lokalizacja	Łacze 1 główne (Mbps) gwarantowana przepustowość	Łącze 2 zapasowe (Mbps) gwarantowana przepustowość	Ilość adresów IP łącze 1	Ilość adresów IP łącze 2	Monitorowanie bezpieczeństwa i aktywna ochrona przed atakami sieciowymi oraz atakami DDoS
1	Toruń, ul. Plac Teatralny 2	**1000**	**400**	255	8	TAK

2	Toruń, ul. Św. Jana 1/3	**100**	-	2	-	-
3	Toruń, ul. Targowa 13-15	**200**	-	2	-	-
4	Toruń, ul. M. Skłodowskiej-Curie 73	**200**	**100**	4	2	-
5	Toruń, ul. Kopernika 4	**100**	-	2	-	-
6	Toruń, Arpol	**300**	**100**	4	2	-
7	Bydgoszcz, ul. Jagiellońska 9	**100**	-	2	-	-
8	Bydgoszcz, ul. Gimnazjalna 2a	**100**	-	2	-	-
9	Włocławek, ul. Bechiego 2	**100**	-	8	-	-
10	Grudziądz, ul. Waryńskiego 4	**100**	-	2	-	-
11	Toruń, ul. Franciszkańska 12	**-**	**100**	2	-	-

1) typ łącza: symetryczne;
2) opóźnienia w ramach sieci nie mogą być większe niż 20ms do routera brzegowego
3) łącze nie może posiadać ograniczeń transferu oraz nie może posiadać zablokowanych portów;
4) współczynnik straty pakietów nie większy niż 10^{-3} (zgodnie z zaleceniem ITU-T Y.1541)
5) Łącza nie mogą być zrealizowane w technologii radiowej. Łącza muszą być zrealizowane w technologii światłowodowej.
6) Przepustowość zdefiniowana w tabeli musi być gwarantowana przez Wykonawcę w punktach styku sieci IP Wykonawcy z sieciami IP operatorów Internetowych, z którymi Wykonawca posiada punkty styku.
7) Wykonawca musi posiadać, co najmniej 1 niezależny, bezpośredni punkt styku z Międzynarodowym Dostawcą Internetu.
8) Wykonawca musi posiadać, co najmniej 2 punkty styku z Krajowymi Dostawcami Internetowymi.
9) Wykonawca zabezpieczy przesyłane przez Zamawiającego dane w sposób zgodny z obowiązującymi aktualnie przepisami prawa.
10) Wykonawca musi ściśle współpracować przy aktualizacji i rozpropagowaniu nowych stref DNS Zamawiającego.
11) Nie dopuszcza się zmiany przyznanej adresacji IP w trakcie trwania umowy.
12) Łącze 2 dla lokalizacji wskazanych w tabeli powinno być doprowadzone do budynku inną trasą niż łącze 1:
    a. Oba łącza powinny być zakończone w dwóch różnych węzłach sieci Wykonawcy.
    b. Oba łącza powinny umożliwiać niezależną transmisję danych (tj. dla każdego kanału istnieje redundantny kanał komunikacyjny) poprzez sieć Wykonawcy do dwu różnych węzłów sieci operatora/ów nadrzędnych. Poprzez redundantny kanał rozumie się drugą fizycznie niezależną ścieżkę do innego styku operatora/ów.
    c. Jeśli oba węzły Zamawiającego są podpięte do dwu różnych węzłów tego samego operatora, to dodatkowo należy wykazać, iż te dwa węzły operatora są węzłami w „ringu", a nie „w gałęzi" jego sieci.
    d. Oba łącza z dostępem do Internetu, będą pracować w trybie produkcyjnym

3. **Usługa monitorowania bezpieczeństwa i aktywnej ochrony przed atakami sieciowymi oraz atakami DDoS**:

1) Wykonawca zobowiązuje się, że ochrona przeciw atakom DDoS oraz DoS będzie realizowana sprzętowo na poziomie sieci operatora co najmniej mechanizmami access list, flowspec, blackholing. Wykonawca zapewni też ochronę przed atakami typu flood, sweep, teardrop oraz smurf dla min. protokołów HTTP/HTTPS, FTP, DNS, SIP. 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.
2) Alerty oraz raport w przypadku prób ataków będą przekazywane systematycznie i niezwłocznie na adres: ..... Zmiana adresu, o których mowa w zdaniu poprzedzającym, nie wymaga zmiany Umowy, a jedynie poinformowania drugiej Strony w formie pisemnej. Zawiadomienie takie powinno zostać podpisane przez osoby uprawnione do reprezentacji danej Strony.
3) 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 przez Zamawiającego publicznych adresów IP oraz nie może wiązać się z koniecznością zestawiania dodatkowych tuneli VPN, oraz dodatkowych mechanizmów uwierzytelniania użytkowników opartych o tokeny.
4) Wykonawca zobowiązuje się do przekazania Zamawiającemu raportu każdorazowo po wykrytym i zakończonym ataku DDoS, bezzwłocznie jednak nie później niż w 24 godziny od momentu zakończenia ataku.
   Raport taki powinien zawierać takie dane jak:
   1) Cel ataku (IP i porty celu)
   2) Średnia oraz maksymalna wartość pps i bps
   3) TOP 20 najaktywniejszych źródeł (IP i port źródła)
   4) Geolokalizacja TOP10 źródeł
   5) Wyszczególnienie protokołów wraz z ich flagami z ruchu sieciowego (ICMP, UDP, TCP SYN, TCP ACK, TCP PSH itp.)
5) Zamawiającemu zostanie zapewniony dostęp poprzez jednoczesne logowanie się minimum 5 użytkowników do systemu antyDDoS, przy czym ilość kont użytkowników w systemie antyDDoS wyniesie przynajmniej 5.
6) Wykonawca zobowiązuje się zapewnić Zamawiającemu wsparcie na jego żądanie w trakcie wystąpienia ataku DDoS lub jego podejrzenia (kontakt mailowy i telefoniczny funkcjonujący całodobowo do zespołu technicznego SOC lub inżyniera), polegające na zmianie konfiguracji w systemie antyDDoS mające na celu poprawę ochrony systemów Zamawiającego.
7) Wykonywanie cyklicznych skanów podatności infrastruktury IP z Internetu (raz w miesiącu).
8) Ochrona reputacji - Ochrona domeny przed utratą lub blokadą, przed wykorzystaniem jej w atakach phishingowych.
9) Ochrona poczty, identyfikacja wycieków informacji o pracownikach.
10) Blokowanie podejrzanych stron - Ochrona urządzeń w sieci stacjonarnej, blokada prób komunikacji, które mogą doprowadzić do zainfekowania złośliwym oprogramowaniem
11) Dostarczanie Zamawiającego biuletynów z informacjami o najnowszych cyberzagrozeniach – raz w miesiącu przygotowany materiał który będzie mógł zostać przekazany pracownikom Urzędu Marszałkowskiego w formie biuletynu wewnetrznego.

4. **Dokumentacja powykonawcza.**

1) Wykonawca dostarczy w formie papierowej i elektronicznej dokumentację powykonawczą.

2) Dokumentacja powinna zawierać: schematy podłączenia sieci, informacje o przyznanej puli adresowej dla poszczególnych przyłączy, informacje potrzebnych do konfiguracji routingu do sieci Wykonawcy, informacje o serwerach DNS Dostawcy.

5. **Poziom usług (SLA).**

Poziom świadczonej usługi dostępu do Internetu nie może być niższy niż o poniższych parametrach:

- Gwarantowana data aktywacji usługi, ustalona w umowie,
  - Gwarantowana miesięczna i roczna dostępność usługi na poziomie **min. 99,7% - *zaoferowany poziom dostępności stanowi kryterium dodatkowe***
- Stała przepustowość, zgodnie ze specyfikacją określoną w punkcie 2,
- Gwarantowany czas reakcji na awarię: 1godzina,
- Gwarantowane usunięcie awarii w ciągu 8 godzin od momentu zgłoszenia lub wykrycia awarii przez Wykonawcę,
- Dostępność służb technicznych 24 godziny/dobę, 7 dni w tygodniu przez wszystkie dni w roku,
- Monitorowanie przez Wykonawcę łącza przez 24h/dobę,
- 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. Przez Zgłoszenie rozumie się 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 tym punkcie. W przypadku Zgłoszenia przez więcej niż jeden kanał, chwilą dokonania Zgłoszenia będzie wcześniejsza data i godzina.
- 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.
- W przypadku gdy Wykonawca wykryje Awarię jest zobowiązany do niezwłocznego poinformowania Zamawiającego o jej wystąpieniu poprzez wysłanie wiadomości email oraz usunięcia Awarii w terminie, o którym mowa powyżej.
- Udostepnienie Zamawiającemu dostępu do portalu umożliwiającego monitorowanie usługi dla wszystkich lokalizacji

6. Terminy realizacji:

Uruchomienie usługi dla Łącza 1 – 30-60 dni ***–termin uruchomienia usługi dla łącza 1 stanowi kryterium dodatkowe***

Uruchomienie usługi dla Łącza 2 – 180 dni

7. Wizja lokalna

Zamawiający dopuszcza, aby przed złożeniem oferty Oferenci przeprowadzili wizję lokalną. Przedstawiciel Oferenta indywidualnie na własny koszt i ryzyko przeprowadzi wizję lokalną związaną z przedmiotem zamówienia dla poprawnego przygotowania oferty. Oferent na przeprowadzenie wizji lokalnej ma czas do czasu złożenia oferty. Oferenci zgłaszają swój udział w wizji lokalnej poprzez platformę zakupową Zamawiającego. W trakcie wizji lokalnej zostanie spisana notatka służbowa przez przedstawiciela Zamawiającego, w której zostaną odnotowane: dane uczestników oraz data przeprowadzenia wizji lokalnej.