*Załącznik nr 1 do Rozeznania cenowego*

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia są usługi telekomunikacyjne dla Centrum Egzaminowania   
i Monitorowania Maszynistów (Aleje Jerozolimskie 211, 02-222 Warszawa)

OPIS PARAMETRÓW TECHNICZNYCH I FUNKCJONALNYCH PRZEDMIOTU ZAMÓWIENIA:

1. **Słownik pojęć:**
   1. IP – publiczny adres IP w wersji 4;
   2. Awaria – rozumiana jako przerwa w działaniu Usługi, z wyłączeniem następujących sytuacji:
      1. awaria z przyczyn leżących po stronie Zamawiającego,
      2. brak zasilania, za które winy nie ponosi Wykonawca,
      3. siła wyższa (zdarzenie o charakterze nadzwyczajnym, niemożliwych wcześniej   
         do przewidzenia. Ciężar wskazania zaistniałych okoliczności spoczywa   
         na Wykonawcy),
      4. planowa konserwacja sieci uzgodniona z wyprzedzeniem z Zamawiającym,
      5. brak dostępu do urządzeń i okablowania znajdujących się na powierzchni,   
         do których dostęp zapewnia Zamawiający do których (urządzeń, i okablowania) Wykonawca musi otrzymać dostęp w celu wyeliminowania wadliwego   
         ich działania,
      6. przyczyn leżących po stronie sprzętu i okablowania sieci Zamawiającego nieobjętych Usługą, a także warunków środowiskowych w siedzibie Zamawiającego.
2. **Przedmiotem zamówienia jest świadczenie przez Wykonawcę na rzecz Zamawiającego usług polegających na zapewnieniu usługi symetrycznego dostępu   
   do Internetu wraz z serwisem naprawczym na potrzeby Zamawiającego, zwanej dalej również „Usługą dostępu do Internetu”, obejmujących:**
   1. zestawienie, uruchomienie (wraz z niezbędnym do podłączenia do infrastruktury Zamawiającego sprzętem, w tym urządzeniami teletransmisyjnymi) i udostępnienie przez całą dobę (24 godziny) przez wszystkie dni w roku, stałego symetrycznego łącza dostępowego we wskazanym przez Zamawiającego pomieszczeniu we wskazanej przez Zamawiającego lokalizacji.
3. **Parametry techniczne dla łącza:**
   1. zapewnienie przepustowości gwarantowanej 500 Mb/s,
   2. przyłączenie po stronie Zamawiającego do routerów dostępowych będących   
      w posiadaniu Zamawiającego, za pośrednictwem interfejsów FC, zainstalowanych   
      w urządzeniach StormShield SN2100 pracujących w konfiguracji HA. W związku   
      z tym po stronie Wykonawcy leży dostarczenie przyłącza w takiej formie, by możliwe było wykorzystanie łącza poprzez dowolne z dwóch urządzeń,
   3. cały sprzęt niezbędny do realizacji Usługi dostępu do Internetu dostarczony przez Wykonawcę i zamontowany we wskazanym przez Zamawiającego pomieszczeniu,
   4. dostęp do wszystkich usług i serwisów internetowych krajowych i zagranicznych,
   5. nielimitowana ilość sesji oraz przesyłanych danych, z zastrzeżeniem, że wymaganie   
      to nie dotyczy blokowania ruchu związanego ze zidentyfikowanymi przez Wykonawcę atakami skierowanymi na infrastrukturę Zamawiającego lub blokowania adresacji   
      IP pojedynczych adresów IP bądź całych sieci internetowych (ograniczonych maską   
      – dowolną) przekazanej przez Zamawiającego,
   6. obsługę adresów IP używanych przez Zamawiającego, przydzielonych przez Wykonawcę w ramach świadczenia usługi,
   7. obsługę zgłoszeń w zakresie problemów eksploatacyjnych przez 24 godziny na dobę przez wszystkie dni w roku,
   8. świadczenie usługi wsparcia technicznego na rzecz wszystkich upoważnionych administratorów Zamawiającego (do 6 osób),
   9. przydzielenia minimum 30 publicznych adresów IPv4 (maska /27),   
      nie występujących na ogólnodostępnych w sieci Internet czarnych listach (IP Address Blacklist),
   10. blokowania adresacji IP przekazanej przez Zamawiającego. Wymóg blokowania   
       na wskazanych przez Zamawiającego łączach internetowych adresów IP bądź całych sieci internetowych (ograniczonych maską – dowolną) na wyraźne każdorazowe   
       (bez limitów czasowych, ilościowych) żądanie Zamawiającego. Blokowanie realizowane na urządzeniach dostępowych Wykonawcy,
   11. wykonawca umożliwi Zamawiającemu ustawienie reverse DNS dla poszczególnych adresów IP nazw domen dla których Zamawiający jest subskrybentem,
   12. wykonawca zagwarantuje dla usługi roczną dostępność na poziomie od 99,5%   
       do 99,9% (uwaga – parametr deklarowany przez Wykonawcę jako % dostępności   
       w podanym przedziale z dokładnością do 0,1 i jest kryterium uwzględnianym przy wyborze najkorzystniejszej oferty), czas usunięcia Awarii od momentu zgłoszenia nie może dłuższy niż 4 godzin,
   13. usługa ochrony przed atakami Distributed Denial of Service (DDoS) dla całej udostępnionej przepustowości oferowanego łącza i dla całej adresacji IP Zamawiającego obejmująca:
       1. monitorowanie ruchu sieciowego kierowanego do sieci Zamawiającego   
          pod kątem prób ataków DDoS na udostępnione usługi w trybie 24/7/365   
          z ukierunkowaniem na wykrycie anomalii mogących skutkować wysyceniem łącza i utratą ciągłości procesów biznesowych,
       2. monitoring odbywający się wyłącznie na urządzeniach Wykonawcy   
          bez przekierowywania ruchu poza teren (granice) Rzeczpospolitej Polskiej. Monitoringiem i obsługą incydentów związanych z atakami musi zajmować   
          się wyspecjalizowana jednostka realizująca funkcję wyłącznie nadzoru pracująca w sposób ciągły (24/7/365),
       3. linię wsparcia, która będzie pełnić funkcję monitoringu i operacyjnej ochrony przed atakami oraz prowadzić ciągły dyżur,
       4. linię wsparcia (niezależną od linii wymienionej w punkcie poprzednim),   
          która będzie realizowała funkcję poszukiwania i wdrażania niestandardowych rozwiązań związanych z obsługą incydentów bezpieczeństwa,
       5. ochronę przed wolumetrycznymi atakami DDoS,
       6. ochronę co najmniej przed następującymi typami ataków: TCP SYN flood, UDP flood HTTP GET flood, HTTP POST flood, ICMP flood, IGMP flood, invalid packets, IP fragments, IP NULL, DNS flood, SIP request flood, SSL negotiation,
       7. zapobieganie atakom do przepływności 10 Gbps,
       8. powiadamianie Zamawiającego (poprzez ustalone kanały komunikacji)   
          w ciągu 15 minut od pojawienia się zagrożeń wskazujących na wystąpienie ataku DDoS,
       9. przekierowywanie ruchu w przypadku podejrzenia wystąpienia ataku   
          do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy, zlokalizowanych na terytorium Rzeczpospolitej Polskiej, w ciągu 20 minut   
          od zgłoszenia przez Zamawiającego. Brak przekierowania ruchu po upływie   
          ww. 20 minut będzie traktowane jako Awaria,
       10. zastosowanie filtrowania ruchu za pomocą „blacklist” oraz „whitelist”   
           w czasie nie dłuższym niż 2 godziny od wykrycia incydentu,
       11. filtrowanie ruchu sieciowego (odrzucanie pakietów pochodzących   
           ze źródeł ataku, zanim właściwy ruch zostanie przekazany   
           do Zamawiającego) przy możliwie jak najmniejszym wpływie na ruch uprawniony oraz przekierowywanie odfiltrowanego ruchu   
           do Zamawiającego,
       12. dostęp dla Zamawiającego do panelu usługi DDoS za pośrednictwem którego będzie możliwość pełnego monitoring systemu ochrony DDoS,
       13. przyjmowanie wnioskowanych przez Zamawiającego zmian parametrów usługi systemu ochrony DDoS oraz ich implementację po wcześniejszym skonsultowaniu ze specjalistami Zamawiającego, że wdrażane zmiany   
           nie spowodują negatywnych skutków dla funkcjonowania łącza internetowego Zamawiającego,
       14. przygotowanie dla Zamawiającego raportu po zakończeniu oczyszczania ruchu po zaistniałym ataku DDoS.