

### OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest **zestawienie wraz z niezbędnymi urządzeniami, uruchomienie oraz świadczenie usługi dostępu do sieci Internet przy wykorzystaniu łączy światłowodowych w Serwerowni Centralnej** (zwanej dalej „Serwerownią”) Centrum e-Zdrowia (zwanym dalej „Zamawiającym”) w Warszawie.

#### I. Przedmiot zamówienia obejmuje:

- Etap I - Doprowadzenie łączy światłowodowych do Serwerowni zlokalizowanej w Warszawie przy ul. Stanisława Dubois 5A oraz konfiguracje niezbędnych urządzeń.
- Etap II - Uruchomienie i świadczenie usługi dostępu do Internetu z zachowaniem wymaganych parametrów usługi oraz czasów usunięcia awarii, jak również zapewnienie usługi ochrony przed atakami DDoS.

#### II. Wykonawca zobowiązuje się do realizacji Przedmiotu Umowy (Etap I i II) z zastrzeżeniem, że:

- Etap I zostanie rozpoczęty najwcześniej dnia 1 marca 2023 r., a zakończony najpóźniej dnia 15 marca 2023 r. Do dnia 15 marca 2023 r. zostaną zakończone testy opisane w pkt. 12 tabeli poniżej.
- Etap II zostanie rozpoczęty dnia 1 kwietnia 2023 r. o godzinie 00:00, a zakończony najpóźniej dnia 31 marca 2025 r. o godzinie 23:59. W ramach Prawa Opcji Zamawiający przewiduje przedłużenie Umowy do dnia 31 marca 2026 r. - zamówienie opcjonalne

#### III. Szczegółowe wymagania dotyczące parametrów świadczenia usługi dostępu do Internetu:

1.	<b>Technologia transmisji danych</b>	Usługa dostępu do Internetu ma być świadczona w oparciu o łączy światłowodowe zakończone interfejsem na routerze brzegowym w Serwerowni zlokalizowanej w Warszawie przy ul. Stanisława Dubois 5A.
2.	<b>Gwarantowana przepustowość łączy</b>	Co najmniej 2000 Mbit/s – łączy symetryczne bez limitu transferu danych, nielimitowaną ilość otwartych sesji, brak blokowania usług i protokołów w Internecie. Zamawiający zastrzega sobie, że w trakcie trwania Umowy może zgłosić zapotrzebowanie na inną wartość łączy światłowodowych, dla gwarantowanej przepustowości łączy co najmniej 4000 Mbit/s z wyprzedzeniem co najmniej 10 dni przed rozpoczęciem nowego miesiąca kalendarzowego.
3.	<b>Dostępność usługi</b>	3.1 min. 99,5 % – łączny czas niedostępności usługi w ciągu roku może wynieść maksymalnie 48 godzin. 3.2 min. 99,5 % - łączny czas niedostępności usługi w ciągu miesiąca wyniesie maksymalnie 4 godziny.

4.	<b>Interfejsy</b>	Połączenie do sieci Internet oraz do sieci wewnętrznej Zamawiającego musi wykorzystywać odrębne interfejsy na routerze brzegowym w Serwerowni.
5.	<b>Adresy IP i parametry sesji</b>	<p>5.1 Obsługa ruchu generowanego przez Zamawiającego przy pomocy dynamicznego protokołu routingu BGP (Border Gateway Protocol) w wersji 4.</p> <p>5.2 Wykonawca zapewni obsługę adresów IPv4 PI (Provider Independent) 109.197.164.0/24 oraz numeru AS 199105 przypisanych w RIPE do Zamawiającego.</p> <p>5.3 Wykonawca w czasie realizacji usługi zapewni na potrzeby Zamawiającego 64 adresy publiczne IPv4 wydzielone ze swojej puli (adresy typu PA).</p> <p>5.4 Sesja BGP umożliwiająca automatyczne przełączenie w tryb aktywny w przypadku awarii zapasowego łącza radiowego w Serwerowni obsługiwanego przez odrębnego Operatora Telekomunikacyjnego.</p> <p>5.5 Konfiguracja routerów umożliwiająca automatyczne przejęcie obsługi ruchu z sieci Zamawiającego w przypadku awarii bramy domyślnej jednego z routerów.</p>
6.	<b>Serwer DNS</b>	<p>Zapewnienie oraz utrzymanie serwera secondary DNS dla domen:</p> <ul style="list-style-type: none"> <li>• cez.gov.pl</li> <li>• csioz.gov.pl</li> <li>• mz.gov.pl</li> <li>• smwk.gov.pl</li> <li>• ezdrowie.gov.pl</li> <li>• zdrowie.gov.pl</li> <li>• e-recepta.gov.pl</li> <li>• ikp.gov.pl</li> <li>• pacjent.gov.pl</li> <li>• inwestycjewzdrowie.gov.pl</li> <li>• opiekacalodobowa.gov.pl</li> <li>• gabinet.gov.pl</li> <li>• zoz.org.pl</li> <li>• akademiacez.gov.pl</li> <li>• planujedlugiezycie.pl</li> </ul>
7.	<b>Routery brzegowe</b>	<p>Wykonawca uruchomi, skonfiguruje i wdroży do pracy dwa routery będące własnością Zamawiającego.</p> <p>Zamawiający dysponuje routerami CISCO C8500L-8S4X.7.2 Routery muszą pracować w konfiguracji redundantnej odpornej na awarię bramy domyślnej dla ruchu do i z sieci Zamawiającego. Routery muszą być skonfigurowane do obsługi protokołu BGP. Administracja routerami pozostaje po stronie CeZ.</p>

8.	<b>Obsługa awarii</b>	<p>8.1 Wykonawca ma zapewnić gotowość przyjmowania zgłoszeń awarii oraz nieprawidłowości funkcjonowania świadczonej usługi 24 godziny na dobę przez 365 dni w roku.</p> <p>8.2 Gwarantowany czas reakcji – max. 1 godzina od wystąpienia zgłoszenia, przyjmowanie zgłoszeń przez e-mail lub poprzez portal Wykonawcy w trybie 24/7 przez 365 dni w roku.</p> <p>8.3 Gwarantowany czas usunięcia awarii – max. 4 godziny od momentu potwierdzenia przyjęcia zgłoszenia, usuwanie awarii w trybie 24/7 przez 365 dni w roku.</p>
9.	<b>Wsparcie Wykonawcy</b>	<p>9.1 W całym okresie trwania umowy usuwanie awarii oraz nieprawidłowości w funkcjonowaniu świadczonej usługi dostępu do sieci Internet.</p> <p>9.2 W całym okresie trwania umowy rozwiązywanie problemów sprzętowych i konfiguracyjnych dostarczonych urządzeń realizujących usługę dostępu do sieci Internet.</p> <p>9.3 Wykonawca na czas trwania umowy dostarczy zainstaluje oraz skonfiguruje wszystkie niezbędne urządzenia do realizacji usługi wraz z niezbędnym okablowaniem.</p> <p>9.4 Wykonawca zestawi i uruchomi łącze dostępowe do sieci Internet w Serwerowni.</p> <p>9.5 Wykonawca będzie współpracował z Operatorem zapasowego łącza radiowego w celu skonfigurowania wszelkich parametrów dla sesji BGP oraz konfiguracji routera brzegowego.</p>
10.	<b>Ochrona przed atakami DDoS</b>	<p>10.1 Zamawiający wymaga zapewnienia usługi ochrony przed atakami DDoS w tym atakami wolumetrycznymi dla całej udostępnianej przepustowości łącza.</p> <p>10.2 Zamawiający wymaga aby ochrona przed atakami DDoS realizowana była w sposób proaktywny na urządzeniach w sieci Wykonawcy bez przekierowywania ruchu poza teren Rzeczypospolitej Polskiej.</p> <p>10.3 W momencie wystąpienia ataku DDoS, system realizujący usługę ma wykonać mechanizm mitygacji ataku a następnie do sieci Zamawiającego ma trafić oczyszczony ruch wpływu na działanie usługi dostępu do Internetu. Zamawiający wymaga wdrożenia dodatkowej funkcjonalności polegającej na przekierowaniu ruchu do atakowanego adresu przez dodatkowy serwer filtrujący (przekierowanie będzie aktywne tylko w trakcie trwania ataku), który odrzuci cały ruch z adresów innych niż Polskie.</p> <p>10.4 Usługa powinna monitorować ruch do sieci Zamawiającego w czasie rzeczywistym oraz zapewniać ochronę przed co najmniej następującymi typami ataków: TCP SYN flood, UDP</p>

		<p>flood, DNS reflection, DNS flood, HTTP GET flood, HTTP POST flood, ICMP flood.</p> <p>10.5 System realizujący usługę ma samodzielnie wykrywać anomalie polegające na znaczącym przekroczeniu wolumenu ruchu oraz ataki na usługi Zamawiającego wystawione pod publicznymi adresami IP na podstawie danych historycznych z ruchu sieciowego wyznaczanych w trakcie realizacji usługi.</p>
<b>11.</b>	<b>Dodatkowe wymagania</b>	<p>11.1 Wykonawca ma posiadać, co najmniej 3 niezależne, bezpośrednie punkty styku z Międzynarodowymi Dostawcami Internetowymi o przepustowości min. 1 Gb/s każdy.</p> <p>11.2 Wykonawca ma posiadać, co najmniej 3 punkty styku z Krajowymi Dostawcami Internetowymi o przepustowości min. 1 Gb/s każdy.</p> <p>11.3 Wykonawca ma uczestniczyć w co najmniej dwóch Punktach Wymiany Ruchu Internetowego – Internet Exchange (np. WIX, PL-IX).</p> <p>11.4 Wykonawca dokona wszelkich ustaleń z administratorami i służbami technicznymi budynku, w którym świadczona będzie usługa na własny koszt.</p>
<b>12.</b>	<b>Testy</b>	<p>12.1 Po doprowadzeniu łącza światłowodowego do Serwerowni oraz montażu i konfiguracji niezbędnych urządzeń w ramach Etapu I, w ciągu 3 dni roboczych zostaną wykonane testy potwierdzające:</p> <ul style="list-style-type: none"> <li>• Przepustowość łącza</li> <li>• Poprawność przełączania sesji BGP</li> <li>• Przełączanie bramy domyślnej za pomocą VRRP</li> </ul>
<b>13.</b>	<b>Instrukcja techniczna z ochrony przed atakami DDoS</b>	<p>Wykonawca zapewni dla min. 3 osób wskazanych do realizacji Umowy po stronie Zamawiającego uczestnictwo w dedykowanym instruktażu technicznym z zakresu aspektów ochrony przed atakami DDoS realizowanym na potrzeby usługi dostarczonej dla Zamawiającego.</p> <p>Instrukcja techniczna będzie trwać przynajmniej 8 godzin i zostanie przeprowadzony w siedzibie Zamawiającego z zastrzeżeniem, że Zamawiający zobowiązuje się do zapewnienia sali oraz nieprzerwanego w czasie trwania instruktażu oddelegowania 2 pracowników. Instrukcja techniczna ma zostać przeprowadzony w terminie uzgodnionym z Zamawiającym w ramach Etapu I zamówienia, przed jego końcowym odbiorem.</p>