1 Wstęp

1.1 Cel zamówienia

Celem niniejszego zamówienia jest zapewnienie stałego, niezawodnego i bezpiecznego dostępu do Internetu dla Urzędu Zamówień Publicznych w siedzibie przy ul. Postępu 17A, 02-676 Warszawa. Zamówienie obejmuje dwa niezależne łącza: podstawowe (światłowodowe) oraz zapasowe (radiowe), każde z pełną ochroną AntyDDoS oraz usługami DNS. Realizacja zamówienia ma na celu zapewnienie ciągłości pracy Urzędu, wysokiej dostępności usług teleinformatycznych oraz bezpieczeństwa transmisji danych.

1.2 Podział zamówienia na części

Zamówienie zostało podzielone na dwie części:

- **Część 1 – Łącze podstawowe (światłowodowe):** zapewniające główny dostęp do Internetu.
- **Część 2 – Łącze zapasowe (radiowe):** zapewniające awaryjny dostęp do Internetu w przypadku niedostępności łącza podstawowego.

Każda część może być realizowana przez innego wykonawcę. Zamawiający wymaga, aby jeden wykonawca mógł złożyć ofertę tylko na jedną część.

1.3 Okres świadczenia usługi

Usługa będzie świadczona przez okres 24 miesięcy, począwszy od 1 listopada 2025 r., z możliwością przedłużenia o kolejny rok w ramach prawa opcji.

1.4 Podstawy prawne zamówienia

Zamówienie prowadzone jest w trybie podstawowym na podstawie ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2024 r. poz. 1320 z późn. zm.). Pojęcia „dostarczania publicznych sieci telekomunikacyjnych", „dostawcy usług" oraz „świadczenia usług telekomunikacyjnych" odnoszą się do ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2023 r. poz. 875 z późn. zm.). Wykonawca musi posiadać wpis do rejestru przedsiębiorców telekomunikacyjnych prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej (UKE) w zakresie obejmującym świadczenie usług światłowodowych lub radiowych.

1.5 Kody CPV i kategorie usług

Przedmiot zamówienia został sklasyfikowany zgodnie z Wspólnym Słownikiem Zamówień (CPV):

- 72400000-4 – Usługi internetowe
- 72411000-4 – Dostawcy usług internetowych

1.6 Wizja lokalna

Zamawiający nie przewiduje obowiązkowej wizji lokalnej przed złożeniem oferty.

2 Część 1 – Łącze podstawowe (światłowodowe)

2.1 Zakres usługi

Przedmiotem części 1 zamówienia jest świadczenie usługi stałego, symetrycznego dostępu do Internetu w trybie 24/7, z wykorzystaniem łącza światłowodowego, zakończonego w serwerowni Urzędu Zamówień Publicznych przy ul. Postępu 17A, 02-676 Warszawa (poziom -1). Usługa obejmuje również ochronę przed atakami DDoS, zapewnienie usług DNS oraz dostarczenie wymaganej puli publicznych adresów IP.

2.2 Wymagania techniczne łącza

- **Przepustowość:** Minimalna gwarantowana przepustowość łącza wynosi 1 Gbps symetrycznie (upload i download), bez limitu transferu danych. Przepustowość musi być gwarantowana (CIR=EIR) zarówno w sieci dostępowej, jak i szkieletowej.
- **Medium transmisyjne:** Łącze musi być zrealizowane w technologii światłowodowej (ciemne włókno), zakończone w szafie rack w serwerowni Zamawiającego. Wykonawca dostarcza i instaluje niezbędne urządzenia brzegowe, zapewniając kompatybilność z przełącznikami Aruba Zamawiającego.
- **Adresacja IP:** Wykonawca przyznaje Zamawiającemu 32 publiczne adresy IP w jednej, nierozłącznej puli adresowej (PI – własność operatora). Adresy muszą być dedykowane wyłącznie Zamawiającemu.
- **Redundancja:** Łącze musi być zabezpieczone protokołem VRRP lub równoważnym mechanizmem przełączania awaryjnego, umożliwiającym automatyczne przełączenie na łącze zapasowe w przypadku awarii.
- **Ograniczenia:** Brak jakichkolwiek limitów transferu, ograniczeń protokołów, blokowania portów czy stosowania proxy/transparency.

2.3 Ochrona przed atakami DDoS

- Wykonawca zobowiązany jest do zapewnienia aktywnej ochrony AntyDDoS dla całego pasma łącza, z automatyczną detekcją i mitygacją ataków wolumetrycznych i aplikacyjnych.

- Minimalne wymagania ochrony:
    - Detekcja i blokowanie ataków typu SYN Flood, UDP Flood, ICMP Flood, HTTP GET/POST Flood.
    - Czas reakcji systemu ochrony: nie dłuższy niż 5 minut od wykrycia ataku.
    - Raportowanie incydentów: każdorazowo po wystąpieniu ataku oraz kwartalnie w formie zbiorczego raportu (zakres: data, czas trwania, typ ataku, zastosowane działania, wpływ na dostępność usługi).

2.4 Usługi DNS

- Wykonawca zapewnia usługę Secondary DNS oraz obsługę revDNS dla przyznanej puli adresów IP.
- Wymagana jest możliwość zarządzania rekordami DNS przez Zamawiającego oraz propagacja wpisów DNS w sieci globalnej.
- Dostępność serwerów DNS: nie mniej niż 90% w miesiącu (zgodnie z tabelą SLA).

2.5 Wymagania dotyczące urządzeń brzegowych i infrastruktury

- Wykonawca dostarcza, instaluje i konfiguruje urządzenia brzegowe niezbędne do świadczenia usługi (np. media konwertery, routery, przełączniki), zapewniając ich kompatybilność z infrastrukturą Zamawiającego.
- Zamawiający zapewnia miejsce w szafie rack (maksymalnie 4U), zasilanie (w tym awaryjne – UPS) oraz chłodzenie.
- Urządzenia brzegowe muszą być objęte serwisem on-site z gwarantowanym czasem naprawy nie dłuższym niż 3 godziny od zgłoszenia awarii.

2.6 Instalacja i dostęp do budynku

- Instalacja łącza i urządzeń może być realizowana wyłącznie w obecności pracownika Zamawiającego oraz po wcześniejszym uzgodnieniu z zarządcą budynku Adgar.
- Prace instalacyjne mogą być prowadzone w godzinach popołudniowych (po 16:00) oraz w weekendy, zgodnie z wytycznymi zarządcy budynku.
- Wykonawca jest zobowiązany do przestrzegania przepisów BHP, ppoż. oraz wytycznych organizacyjnych Adgar Plaza.
- W przypadku nieudanej konfiguracji lub awarii podczas instalacji, Wykonawca zobowiązany jest do przywrócenia stanu pierwotnego (działającego łącza) do końca okresu instalacyjnego (maksymalnie od piątku do niedzieli).

2.7 Monitoring, raportowanie i SLA

- Wykonawca zapewnia monitoring dostępności i przepustowości łącza.
- Raportowanie: kwartalne raporty obejmujące dostępność usługi, incydenty bezpieczeństwa (DDoS), zgłoszenia awarii i czas ich usunięcia, dostępność DNS, wykorzystanie adresacji IP.
- SLA:
    - Dostępność usługi: ≥99% – 100% opłaty, 95–99% – 75%, <95% – 0%.
    - Czas reakcji na zgłoszenie: maksymalnie 1 godzina.
    - Czas przywrócenia dostępności: maksymalnie 3 godziny.
    - Dostępność DNS: ≥90% – 100% opłaty, 80–90% – 75%, 70–80% – 50%, <70% – 0%.

2.8 Testy odbiorcze i dokumentacja powykonawcza

- Po zakończeniu instalacji Wykonawca przeprowadzi testy odbiorcze, obejmujące:
    - Test przepustowości (za pomocą narzędzia speedtest.pl) – wynik nie niższy niż 950 Mbps w obu kierunkach.
    - Test failover (przełączenie na łącze zapasowe i powrót).
    - Test dostępności usług DNS i AntyDDoS.
- Wykonawca zobowiązany jest do przekazania dokumentacji powykonawczej obejmującej schematy połączeń, instrukcje obsługi urządzeń brzegowych, protokoły pomiarowe oraz protokół odbioru podpisany przez obie strony.

2.9 Bezpieczeństwo i zgodność

- Wykonawca musi posiadać wpis do rejestru przedsiębiorców telekomunikacyjnych UKE (zakres: światłowód) oraz certyfikat ISO 27001.
- Wymagane jest posiadanie własnego centrum monitoringu sieci (NOC/SOC) na terenie Polski, czynnego 24/7.
- Wszelkie prace instalacyjne muszą być wykonywane przez osoby z aktualnymi uprawnieniami SEP/BHP.

2.10 Prawo opcji

- Zamawiający przewiduje prawo opcji na rozszerzenie puli adresów IP o maksymalnie 30 dodatkowych adresów w trakcie trwania umowy.

- Procedura zamówienia dodatkowych adresów: pisemne zgłoszenie przez Zamawiającego, realizacja w terminie do 14 dni, rozliczenie według stawki jednostkowej określonej w ofercie.

2.11 Inne wymagania

- Usługa musi być świadczona wyłącznie na własnej infrastrukturze wykonawcy.
- Zamawiający dopuszcza świadczenie usług w modelu cross-connect z innym operatorem obecnym w budynku.
- Wymagane jest wsparcie dla protokołu IPv6 (w przypadku wdrożenia przez Zamawiającego w przyszłości).
- Wszelkie prace i usługi muszą być zgodne z normami branżowymi MEF oraz ITU-T.

3 Część 2 – Łącze zapasowe (radiowe)

3.1 Zakres usługi

Przedmiotem części 2 zamówienia jest świadczenie usługi stałego, symetrycznego dostępu do Internetu w trybie awaryjnym (łącze zapasowe) z wykorzystaniem łącza radiowego, zakończonego w serwerowni Urzędu Zamówień Publicznych przy ul. Postępu 17A, 02-676 Warszawa (poziom -1). Usługa obejmuje również ochronę przed atakami DDoS, zapewnienie usług DNS oraz dostarczenie wymaganej puli publicznych adresów IP.

3.2 Wymagania techniczne łącza

- **Przepustowość:** Minimalna gwarantowana przepustowość łącza wynosi 800 Mbps symetrycznie (upload i download), bez limitu transferu danych. Przepustowość musi być gwarantowana (CIR=EIR) zarówno w sieci dostępowej, jak i szkieletowej.
- **Medium transmisyjne:** Łącze musi być zrealizowane w technologii radiowej punkt-punkt, w paśmie licencjonowanym. Wykonawca zobowiązany jest do przedstawienia kopii decyzji rezerwacyjnej UKE na wykorzystywane pasmo radiowe przed rozpoczęciem instalacji.
- **Adresacja IP:** Wykonawca przyznaje Zamawiającemu nie mniej niż 32 publiczne adresy IP w jednej, nierozłącznej puli adresowej (PI – własność operatora). Adresy muszą być dedykowane wyłącznie Zamawiającemu.
- **Redundancja:** Łącze zapasowe pracuje w trybie cold standby – aktywowane tylko w przypadku awarii łącza podstawowego. Przełączenie ruchu na łącze

zapasowe musi odbywać się automatycznie (np. VRRP, BGP failover) w czasie nie dłuższym niż 60 sekund od wykrycia awarii.

- **Ograniczenia:** Brak jakichkolwiek limitów transferu, ograniczeń protokołów, blokowania portów czy stosowania proxy/transparency.

3.3 Wymagania dotyczące urządzeń radiowych i instalacji

- Urządzenia radiowe muszą być odporne na warunki atmosferyczne, posiadać zabezpieczenia przed przepięciami i być zamontowane zgodnie z wytycznymi producenta oraz zarządcy budynku.
- Minimalny poziom sygnału RSSI na obu końcach łącza nie może być niższy niż -65 dBm.
- Minimalna odporność na temperaturę: od -30°C do +60°C, wilgotność względna: do 95% bez kondensacji, stopień ochrony IP: co najmniej IP65.
- Urządzenia muszą posiadać zabezpieczenia przeciwprzepięciowe, wsparcie dla SNMP v2/v3, możliwość zdalnego zarządzania.
- Zamawiający zapewnia miejsce w szafie rack (4U), zasilanie (w tym awaryjne – UPS) oraz chłodzenie.
- Wykonawca zobowiązany jest do przedstawienia dokumentacji powykonawczej: schematy połączeń, zdjęcia instalacji, certyfikaty zgodności, protokoły pomiarowe, instrukcje obsługi, protokół odbioru.

3.4 Ochrona przed atakami DDoS

- Wykonawca zobowiązany jest do zapewnienia aktywnej ochrony AntyDDoS dla całego pasma łącza, z automatyczną detekcją i mitygacją ataków wolumetrycznych i aplikacyjnych.
- Minimalne wymagania ochrony: detekcja i blokowanie ataków typu SYN Flood, UDP Flood, ICMP Flood, HTTP GET/POST Flood.
- Czas reakcji systemu ochrony: nie dłuższy niż 5 minut od wykrycia ataku.
- Raportowanie incydentów: każdorazowo po wystąpieniu ataku oraz kwartalnie w formie zbiorczego raportu (zakres: data, czas trwania, typ ataku, zastosowane działania, wpływ na dostępność usługi).

3.5 Usługi DNS

- Wykonawca zapewnia usługę Secondary DNS oraz obsługę revDNS dla przyznanej puli adresów IP.

- Wymagana jest możliwość zarządzania rekordami DNS przez Zamawiającego oraz propagacja wpisów DNS w sieci globalnej.
- Dostępność serwerów DNS: nie mniej niż 90% w miesiącu (zgodnie z tabelą SLA).

3.6 Tryb pracy łącza zapasowego

- Łącze zapasowe pracuje w trybie cold standby – aktywowane tylko w przypadku awarii łącza podstawowego.
- Przełączenie ruchu na łącze zapasowe musi odbywać się automatycznie (np. VRRP, BGP failover) w czasie nie dłuższym niż 60 sekund od wykrycia awarii.
- Po przywróceniu dostępności łącza podstawowego ruch powinien być automatycznie przełączony z powrotem na łącze podstawowe bez utraty sesji krytycznych.

3.7 Testy failover i odbiorcze

- Wykonawca zobowiązany jest do przeprowadzenia testów przełączenia/failover podczas odbioru usługi oraz okresowo, nie rzadziej niż raz na pół roku w trakcie trwania umowy.
- Scenariusz testów failover:
    - Symulacja awarii łącza podstawowego.
    - Automatyczne przełączenie ruchu na łącze zapasowe w czasie nie dłuższym niż 60 sekund.
    - Test przepustowości (wynik nie niższy niż 750 Mbps w obu kierunkach).
    - Test powrotu do normalnej pracy (przełączenie na łącze podstawowe).
    - Brak utraty sesji krytycznych (np. VPN, VoIP, aplikacje biznesowe).

3.8 Wymagania dotyczące serwisu i wsparcia

- Zgłoszenia awarii przyjmowane są przez dedykowany numer telefonu oraz portal zgłoszeniowy 24/7.
- Potwierdzenie przyjęcia zgłoszenia w ciągu 15 minut, status zgłoszenia dostępny online.
- W przypadku awarii sprzętu radiowego, Wykonawca zobowiązany jest do podjęcia działań serwisowych on-site w ciągu 2 godzin od zgłoszenia oraz do przywrócenia pełnej funkcjonalności w ciągu maksymalnie 6 godzin.

- W przypadku wdrożenia przez Zamawiającego systemu monitoringu lub SIEM, Wykonawca zobowiązuje się do udostępnienia interfejsu API lub SNMP do integracji.

3.9 Wymagania dotyczące wsparcia dla IPv6

- Wykonawca zobowiązuje się do zapewnienia wsparcia dla IPv6 w terminie 30 dni od pisemnego zgłoszenia przez Zamawiającego, bez dodatkowych opłat za aktywację protokołu.

3.10 Raportowanie i dokumentacja

- Raporty kwartalne w formacie PDF i XLSX, zakres: dostępność, awarie, testy failover, wykorzystanie IP, incydenty bezpieczeństwa, rekomendacje.
- Dokumentacja powykonawcza obejmuje: schematy połączeń, zdjęcia instalacji, certyfikaty zgodności, protokoły pomiarowe, instrukcje obsługi, protokół odbioru.

4 Wymagania wspólne dla obu części

4.1 Warunki świadczenia usług

1. **Ciągłość i niezawodność:** Usługi muszą być świadczone w trybie 24/7/365, z zachowaniem wysokiej dostępności i niezawodności, zgodnie z wymaganiami SLA określonymi w niniejszym OPZ.
2. **Gwarantowana przepustowość:** Wymagana jest gwarantowana przepustowość (CIR=EIR) zarówno dla łącza podstawowego, jak i zapasowego, bez limitów transferu danych i ograniczeń protokołów.
3. **Adresacja IP:** Wykonawca zapewnia Zamawiającemu nie mniej niż 32 publiczne adresy IP (PI – własność operatora) w jednej, nierozłącznej puli adresowej dla każdej części. Adresy muszą być dedykowane wyłącznie Zamawiającemu.
4. **Usługi DNS:** Wykonawca zapewnia usługę Secondary DNS oraz obsługę revDNS dla przyznanej puli adresów IP, z możliwością zarządzania rekordami przez Zamawiającego.
5. **Ochrona AntyDDoS:** Wykonawca zapewnia aktywną ochronę AntyDDoS dla całego pasma każdej części, z automatyczną detekcją i mitygacją ataków oraz raportowaniem incydentów.

4.2 Sposób zgłaszania awarii i kontakt serwisowy

1. **Kanały zgłoszeń:** Zgłoszenia awarii i incydentów przyjmowane są przez dedykowany numer telefonu oraz portal zgłoszeniowy dostępny 24/7.

Potwierdzenie przyjęcia zgłoszenia następuje w ciągu 15 minut, a status zgłoszenia jest dostępny online.

2. **Czas reakcji i naprawy:** Maksymalny czas reakcji na zgłoszenie awarii wynosi 1 godzinę dla łącza podstawowego i 15 minut dla łącza zapasowego. Maksymalny czas przywrócenia pełnej funkcjonalności wynosi odpowiednio 3 godziny (światłowód) i 6 godzin (radiolinia).
3. **Serwis on-site:** W przypadku awarii wymagającej interwencji na miejscu, Wykonawca zobowiązany jest do podjęcia działań serwisowych on-site w ciągu 2 godzin od zgłoszenia.

4.3 Monitoring, raportowanie i SLA

1. **Monitoring:** Wykonawca zapewnia monitoring dostępności, przepustowości, usług DNS oraz ochrony AntyDDoS dla obu części. W przypadku wdrożenia przez Zamawiającego systemu monitoringu lub SIEM, Wykonawca zobowiązuje się do udostępnienia interfejsu API lub SNMP do integracji.
2. **Raportowanie:** Wykonawca zobowiązany jest do przekazywania Zamawiającemu kwartalnych raportów w formacie PDF i XLSX, obejmujących:
    - Dostępność usług,
    - Zgłoszone i usunięte awarie,
    - Wyniki testów failover,
    - Wykorzystanie adresów IP,
    - Incydenty bezpieczeństwa (w tym DDoS),
    - Rekomendacje dotyczące poprawy jakości usług.
3. **SLA:** Dostępność usług, czasy reakcji i naprawy oraz dostępność DNS rozliczane są zgodnie z tabelami SLA opisanymi w rozdziałach dotyczących poszczególnych części. Prace planowe (okna serwisowe) muszą być zgłaszane z co najmniej 7-dniowym wyprzedzeniem i uzgadniane z Zamawiającym.

4.4 Wymagania dotyczące instalacji i dokumentacji

1. **Instalacja:** Wszystkie prace instalacyjne muszą być wykonywane zgodnie z wytycznymi zarządcy budynku Adgar oraz w obecności pracownika Zamawiającego. Prace mogą być prowadzone w godzinach popołudniowych i w weekendy, zgodnie z ustaleniami.
2. **Dokumentacja powykonawcza:** Po zakończeniu instalacji Wykonawca zobowiązany jest do przekazania Zamawiającemu dokumentacji powykonawczej, obejmującej:

- Schematy połączeń,
- Zdjęcia instalacji,
- Certyfikaty zgodności,
- Protokoły pomiarowe,
- Instrukcje obsługi urządzeń,
- Protokół odbioru podpisany przez obie strony.

3. **Szkolenie:** Wykonawca przeprowadzi szkolenie dla personelu Zamawiającego z obsługi urządzeń brzegowych i procedur awaryjnych.

4.5 Wymagania dotyczące bezpieczeństwa i zgodności

1. **Rejestr UKE:** Wykonawca musi posiadać ważny wpis do rejestru przedsiębiorców telekomunikacyjnych prowadzonego przez Prezesa UKE, obejmujący świadczenie usług światłowodowych i/lub radiowych.
2. **Certyfikaty:** Wykonawca musi posiadać certyfikat ISO 27001 oraz własne centrum monitoringu sieci (NOC/SOC) na terenie Polski, czynne 24/7.
3. **Uprawnienia personelu:** Wszystkie prace instalacyjne muszą być wykonywane przez osoby z aktualnymi uprawnieniami SEP/BHP.
4. **Ochrona danych osobowych:** W ramach realizacji umowy nie będą przetwarzane dane osobowe Zamawiającego ani jego klientów.

4.6 Wymagania dotyczące prawa opcji i rozbudowy

1. **Prawo opcji:** Zamawiający przewiduje prawo opcji na rozszerzenie puli adresów IP o maksymalnie 30 dodatkowych adresów w trakcie trwania umowy. Zamówienie dodatkowych adresów następuje na pisemny wniosek Zamawiającego, realizacja w terminie do 14 dni, rozliczenie według stawki jednostkowej określonej w ofercie.
2. **Rozbudowa przepustowości:** Zamawiający nie przewiduje możliwości rozbudowy przepustowości łącza w trakcie trwania umowy.

4.7 Wymagania dotyczące odbioru i testów

1. **Testy odbiorcze:** Po zakończeniu instalacji Wykonawca przeprowadzi testy odbiorcze obejmujące:
   - Test przepustowości (światłowód: min. 950 Mbps, radiolinia: min. 750 Mbps w obu kierunkach),
   - Test failover (przełączenie na łącze zapasowe i powrót),

- Test dostępności usług DNS i AntyDDoS.

2. **Testy okresowe:** Testy failover muszą być przeprowadzane nie rzadziej niż raz na pół roku w trakcie trwania umowy.
3. **Kryteria pozytywnego odbioru:** Pozytywny odbiór następuje po uzyskaniu wyników testów zgodnych z wymaganiami oraz po podpisaniu protokołu odbioru przez obie strony.

4.8 Wymagania dotyczące fakturowania i rozliczeń

1. **Fakturowanie:** Wykonawca wystawia faktury osobno dla każdej części zamówienia, po zakończeniu każdego miesiąca świadczenia usługi.
2. **Forma faktury:** Zamawiający dopuszcza przesyłanie faktur w formie elektronicznej.
3. **Rozliczenia:** Wynagrodzenie obejmuje wszystkie koszty związane z realizacją usługi, w tym opłaty za adresy IP, ochronę AntyDDoS, serwis, monitoring i raportowanie.

4.9 Wymagania dotyczące norm i standardów

1. **Normy branżowe:** Wszystkie usługi muszą być świadczone zgodnie z obowiązującymi normami branżowymi, w szczególności MEF oraz ITU-T.
2. **Własna infrastruktura:** Usługa musi być świadczona wyłącznie na własnej infrastrukturze wykonawcy, z możliwością świadczenia usług w modelu cross-connect z innym operatorem obecnym w budynku.

5 Załączniki

5.1 Załącznik nr 1 – Schemat połączeń i lokalizacja punktów styku

Schemat połączeń – Łącze podstawowe (światłowodowe) / zapasowe (radiowe)

1. Lokalizacja wejścia do budynku: _____

2. Trasa kabla światłowodowego / lokalizacja anteny radiowej:
_____

3. Lokalizacja szafy rack (poziom -1, serwerownia): _____

4. Porty urządzeń brzegowych (opis, typ, numeracja): _____

5. Opis połączenia z przełącznikiem Zamawiającego: _____

Załącznik graficzny (schemat, zdjęcia): TAK / NIE (dołączyć plik PDF/JPG)

5.2 Załącznik nr 2 – Protokół odbioru instalacji i uruchomienia usługi

Data: _____

Część: [ ] 1 – Łącze podstawowe (światłowodowe) [ ] 2 – Łącze zapasowe (radiowe)

Zakres odbioru:

- Instalacja urządzeń brzegowych: TAK / NIE

- Podłączenie do szafy rack: TAK / NIE

- Konfiguracja adresacji IP: TAK / NIE

- Test przepustowości (wynik): _____ Mbps

- Test failover (czas przełączenia): _____ s

- Test dostępności DNS: TAK / NIE

- Test ochrony AntyDDoS: TAK / NIE

Uwagi i zastrzeżenia: _____

Podpisy:

Przedstawiciel Zamawiającego: _____

Przedstawiciel Wykonawcy: _____

5.3 Załącznik nr 3 – Protokół testów failover i okresowych

PROTOKÓŁ TESTÓW FAILOVER

Data testu: _____

Część: [ ] 1 – Łącze podstawowe [ ] 2 – Łącze zapasowe

Scenariusz testu:

- Symulacja awarii łącza podstawowego: TAK / NIE

- Czas przełączenia na łącze zapasowe: _____ s

- Test przepustowości na łączu zapasowym: _____ Mbps

- Test powrotu do pracy na łączu podstawowym: TAK / NIE

- Utrata sesji krytycznych: TAK / NIE (jeśli TAK, opisać)

Uwagi: _____

Podpisy:

Przedstawiciel Zamawiającego: _____

Przedstawiciel Wykonawcy: _____

5.4 Załącznik nr 4 – Raport kwartalny z realizacji usługi

Okres raportowania: od _____ do _____

1. Dostępność usługi (%): _____

2. Liczba zgłoszonych awarii: _____

3. Średni czas reakcji na zgłoszenie: _____ min

4. Średni czas naprawy: _____ h

5. Wyniki testów failover: _____

6. Wykorzystanie adresów IP: _____

7. Incydenty bezpieczeństwa (opis, data, czas trwania, działania): _____

8. Rekomendacje: _____

Załączniki: [ ] Protokół testów failover [ ] Protokół odbioru [ ] Inne

Podpisy:

Przedstawiciel Wykonawcy: _____

5.5 Załącznik nr 5 – Dokumentacja powykonawcza

Część: [ ] 1 – Łącze podstawowe [ ] 2 – Łącze zapasowe

1. Schematy połączeń: TAK / NIE (załącznik nr ___)
2. Zdjęcia instalacji: TAK / NIE (załącznik nr ___)
3. Certyfikaty zgodności: TAK / NIE (załącznik nr ___)
4. Protokoły pomiarowe: TAK / NIE (załącznik nr ___)
5. Instrukcje obsługi urządzeń: TAK / NIE (załącznik nr ___)
6. Potwierdzenie szkolenia personelu: TAK / NIE (załącznik nr ___)

Podpisy:

Przedstawiciel Wykonawcy: _____

Przedstawiciel Zamawiającego: _____