

## Opis Przedmiotu Zamówienia

### I. Przedmiot zamówienia

1. Przedmiotem zamówienia jest świadczenie usług kolokacyjnych dla posiadanych przez MJWPU serwerów.
2. Rozpoczęcie świadczenia usług kolokacyjnych powinno nastąpić 1.08.2025 i będzie świadczone przez 12 miesięcy.
3. Wykonawca w ramach usługi, przeniesie z obecnej do docelowej lokalizacji serwery MJWPU. Przeniesienie serwerów musi nastąpić przed rozpoczęciem świadczenia usług kolokacyjnych.
4. Przedmiot zamówienia obejmuje:
  - a. Usługę kolokacji infrastruktury informatycznej w centrum danych Wykonawcy
  - b. Usługę przeniesienia konfiguracji z używanych obecnie firewalli na urządzenia zaproponowane w ofercie.
  - c. Usługę relokacji infrastruktury informatycznej do centrum danych Wykonawcy
  - d. Usługę łącza dostępowego do Internetu w centrum danych Zamawiającego
  - e. Usługę udostępnienia urządzeń sieciowych.

### II. Wymagane parametry dla centrum danych Wykonawcy

1. Kolokacja w odległości nie przekraczającej 35 kilometrów od siedziby Zamawiającego (mierzona w linii prostej).
2. Budynek kolokacji musi spełniać normy i standardy minimum zgodnie z normą Tier-3 TIA-942. Wszystkie urządzenia wykorzystywane do realizacji usług muszą posiadać dwa zasilacze redundantne – zgodnie z najlepszymi praktykami rozwiązań Data Center. Nie dopuszcza się stosowania redundancji zasilania z wykorzystaniem dodatkowych urządzeń klasy ATS.
3. Dedykowana szafa minimum 19U przestrzeni dostępnej do użycia (wyłączając listwy zasilające / panele krosownicze / inne stałe elementy, jeżeli ich obecność uniemożliwia montaż standardowego serwera w danym miejscu), minimalne wymiary 1000 mm x 600 mm, zamknięcie co najmniej na zamek mechaniczny.
4. Gwarantowane redundantne zasilanie w obrębie szafy (przynajmniej 2 niezależne obwody zasilające, minimum 22 gniazdka zasilających ISO/IEC C14).
5. Serwerownia zasilana co najmniej z dwóch niezależnych linii energetycznych z podtrzymaniem zasilania przez urządzenia UPS oraz agregat prądotwórczy, zapewniający bezprzerwowe podtrzymanie zasilania w przypadku zaniku napięcia sieciowego.
6. Wartość mocy maksymalnej z tabliczek znamionowych wszystkich zasilanych urządzeń, przy uwzględnieniu redundancji zasilaczy, wynosi 8 kW.
7. Zamawiający wymaga aby energia elektryczna była rozliczana w formie ryczałtu i uwzględniona w miesięcznej opłacie.
8. Fizyczna i techniczna ochrona obiektu serwerowni realizowana w trybie 24 / 7 / 365, w tym wyposażenie serwerowni w automatyczny system ochrony przeciwpożarowej, system kontroli dostępu oraz system monitoringu wizyjnego CCTV działający na zewnątrz oraz w środku serwerowni, zapewniający rejestrację obrazu wraz z datą i godziną oraz zapewniający przechowywanie i dostęp do zarejestrowanych zapisów przez minimum 30 dni.
9. SLA na zasilanie i utrzymanie temperatury w serwerowni nie niższe niż 99,5% liczone w skali miesiąca.

10. Dostęp w ramach serwerowni do klawiatura USB, mysz USB, monitor VGA / DVI / HDMI.

### **III. Wymagania związane z łączem dostępowym do Internetu**

1. Symetryczne łącze do sieci Internet o dostępnej przepustowości co najmniej 500 Mb/s. Łącze do sieci Internet musi być chronione poprzez aplikacyjny system anti-DDoS.
2. Dostęp do sieci Internet musi być zapewniony bez jakichkolwiek limitów czasu dostępu, liczby użytkowników czy też ilości przesłanych lub odebranych danych. Wykonawca zapewni dostęp do wszystkich usług i serwisów internetowych krajowych oraz zagranicznych. Zamawiający wymaga zapewnienia usługi ochrony przed atakami DDoS:
  - a. System musi zapewnić ochronę przeciwko atakom wolumetrycznym oraz wspierać analizę behawioralną (NBA - network behavioral analysis), gdzie jest możliwość zastosowania mechanizmów uczenia specyfiki ruchu oraz detekcji w oparciu o odchylenia parametru "rate" oraz "rate invariant".
  - b. System musi potrafić oczyścić przychodzący ruch Internetowy – dzięki umiejętności uczenia się i rozróżnienia wrogiego ruchu od prawidłowego. Ochrona również musi działać w oparciu o bazę danych reputacji IP (utrzymywanej i aktualizowanej przez producenta rozwiązania)
  - c. System musi działać jako rozwiązanie typu in-line na łączach dedykowanych Internetowych dla Zamawiającego lub jako rozwiązanie klasy scrubbing center sterowane poprzez kontroler bazujący na informacjach o ruchu klasy sFlow/NetFlow lub IPFIX.
  - d. System musi ochraniać przed atakami typu DNS Flood, DNS Random Query, DNS Mirai Flood, HTTP GET/POST Flood, Random Source TCP-SYN Flood, UDP Flood, UDP Fragmented Attack, ICMP Random Flood, Unknown Protocol Flood, PyLoris, Slowloris, Heathbleed, Shellshock, DNS Brute Force, Brute Force HTTP Basic Authentication.
  - e. System musi posiadać możliwość tworzenia list zaufanych adresów IP – wykluczonych z filtrowania.
3. W celu zabezpieczenia przez atakami typu bgp-route-injecting adresacja IP Wykonawcy musi być podpisana cyfrowo poprzez standard RPKI. Dodatkowo wykonawca musi posiadać system śledzenia wystąpień ataku bgp-route-injection w oparciu o analizę globalnych tablic BGP.
4. Przynajmniej 14 stałych adresów IPv4.
5. SLA na dostęp do sieci Internet nie niższe niż 99,5% liczone w skali miesiąca. Na żądanie Zamawiającego, Wykonawca udostępni raport dostępności do sieci Internet.

### **IV. Wymagania związane z przeniesieniem urządzeń Zamawiającego do centrum danych Wykonawcy**

1. Wykonawca w ramach usługi, przeniesie urządzenia Zamawiającego z obecnej lokalizacji do swojego centrum danych.
2. Obecnie urządzenia znajdują się pod adresem: ul. Grochowskiej 21a, 04-186 Warszawa.
3. Przeniesienie urządzeń powinno rozpocząć się najpóźniej w dniu 31.07.2025 i trwać nie dłużej niż 24 godziny. Wykonawca w tym czasie powinien rozłączyć wszystkie połączenia (fiber channel, LAN, zasilanie) i zdemontować urządzenia w obecnej lokalizacji, zabezpieczyć je na czas transportu, przewieźć do swojego centrum danych, zainstalować i odtworzyć połączenia w dedykowanej szafie.
2. Urządzenia zostaną zapakowane w opakowania zastępcze, folie ochronne, antystatyczne, wypełniacze, taśmy, które dostarczy Wykonawca.

3. Opakowanie musi zapewnić zabezpieczenie przed opadami atmosferycznymi, temperaturą i wilgotnością.
4. Przewóz musi być wykonany przez podmiot wyspecjalizowany w zakresie transportu specjalistycznego dysponujący paletami tłumiącymi drgania do przewozu urządzeń elektronicznych, lub z zastosowaniem profesjonalnego sprzętu do relokacji zaprojektowanego do zastosowań uniwersalnych
5. Zamawiający informuje iż urządzenia nie są objęte ubezpieczeniem na wypadek uszkodzenia lub zaginięcia w transporcie. Celem należytego zabezpieczenia interesów Zamawiającego, Wykonawca przedłoży polisę ubezpieczeniową OC z tytułu prowadzonej działalności gospodarczej związanej z Przedmiotem Umowy z sumą gwarantowaną minimum 1 000 000,00 złotych. Wykonawca zobowiązuje się do okazania dowodu posiadania polisy w dniu zawarcia Umowy.
6. W przypadku wystąpienia usterki lub zaginięcia sprzętu, Zamawiający oczekuje, że Wykonawca doprowadzi urządzenia do stanu poprawnego działania, wymieniając uszkodzone lub zaginione komponenty na własny koszt.
7. Naprawa, o której mowa powyżej, powinna zostać wykonana w terminie maksymalnie do 5 dni kalendarzowych od chwili rozpoczęcia przeniesienia urządzeń. Jeżeli Wykonawca nie jest w stanie wykonać naprawy w powyższym terminie, Zamawiający dopuszcza użycie urządzeń zastępczych, o parametrach nie gorszych niż przenoszone urządzenia.
8. Do czasu potwierdzenia przez Zamawiającego poprawności uruchomienia urządzeń i wykonanych konfiguracji, Wykonawca zapewni niezbędne i natychmiastowe wsparcie.
9. Wykaz urządzeń objętych usługą kolokacji:

Urządzenie	Wysokość U	Wartość początkowa
Macierz dyskowa Dell EMC ME5024	2	264 450,00 zł
Serwer Dell EMC PowerEdge R640	1	72 645,03 zł
Serwer Dell EMC PowerEdge R640	1	72 645,03 zł
Serwer Dell EMC PowerEdge R640	1	72 645,03 zł
Macierz dyskowa Dell EMC SCv 3020	3	120 020,94 zł
Switch FC IBM SAN24B-6	1	56 088,00 zł
Switch FC IBM SAN24B-6	1	56 088,00 zł
Switch LAN Brocade ICX7450	1	27 060,00 zł
Switch LAN Brocade ICX7450	1	27 060,00 zł
Serwer Dell EMC PowerEdge R330	1	13 286,46 zł
NAS Synology RS4017 XS+	3	62 976,00 zł
Łączna wartość		844 964,49 zł

#### V. Wymagania związane z firewallem

1. Zamawiający wymaga aby zaproponowane rozwiązanie działało jako klastrer wysokiej dostępności HA.
2. Pojedyncze urządzenie wchodzące w skład klastra, powinno spełniać następujące wymagania:
  - a. musi posiadać minimum 2 porty 10Gbit/s Ethernet oraz minimum dwa dedykowane porty do synchronizacji klastra.
  - b. musi obsługiwać minimum 50000 nowych sesji na sekundę.

- c. musi obsługiwać wydajność dla ruchu z włączoną opcją IPS/ Threat Protection na poziomie minimum 2 Gbps w celu obsługi ruchu wewnętrznego (inter-vlan routing/security).
  - d. musi posiadać wbudowane narzędzie optymalizujące reguły.
  - e. musi wspierać funkcję packet broker'a, gdzie ruch odszyfrowany może zostać wysłany do innego urządzenia bezpieczeństwa – np. systemu ochrony Anti-DDoS
  - f. musi mieć możliwość utworzenia minimum 4 tuneli IPSec S2S oraz minimum 10 połączeń VPN dla użytkowników.
  - g. Możliwość tworzenia użytkowników VPN na urządzeniu Wykonawcy (maksymalnie 50 kont, baza lokalna).
  - h. Inter-VLAN (10 VLAN) dla sieci wewnętrznych z wydajnością nie mniejszą niż 10 Gb/s. Ruch pomiędzy VLAN ma być chroniony przez Firewall'e.
3. Wykonawca zapewni dostęp do panelu administracyjnego, umożliwiającego administrację fizycznym lub wirtualnym firewallem (współdzielonym z innymi klientami Wykonawcy, pod warunkiem zapewnienia pełnej separacji oraz wydajności od sieci innych klientów) oraz bieżący dostęp do logów firewalla.

## **VI. Wymagania związane z konfiguracją firewalla**

- 1. Wykonawca przeprowadzi konfigurację reguł i interfejsów na przydzielonym Zamawiającemu firewallu, która będzie odzwierciedlać aktualną konfigurację na firewallu udostępnionym Zamawiającemu. Zamawiający korzysta z urządzenia typu Next Generation Firewall Palo Alto PA-5220. Aktualne reguły firewall wykorzystują technologię IPSEC VPN, Threat-Prevention, URL Filtering oraz DNS Security. Firewall jest wykorzystywany do ochrony styku z internetem jak i inter-vlan wewnętrznych podsieci Zamawiającego. Firewall musi posiadać aktualne sygnatury i subskrypcje dla podanych funkcji .
- 2. Firewall wydajnościowo musi obsługiwać ruch wewnętrzny jaki i zewnętrzny uwzględniając nieplanowane incydenty takie jak ataki DDoS.
- 3. Wszelkie reguły firewall oraz interfejsy muszą być w osobnym kontekście (VSYS).
- 4. Na podstawie obecnej konfiguracji reguł, Wykonawca dostosuje je do przydzielonej publicznej adresacji IP. Wewnętrzna adresacja oraz nr VLAN, powinny zostać niezmienione.

## **VII. Wymagania związane z audytem centrum danych**

- 1. Wykonawca umożliwi Zamawiającemu przeprowadzenie audytu centrum danych, razy w ciągu trwania Umowy.
- 2. Wykonawca, ze swojej strony, wyznaczy osobę z którą będzie się porozumiewał z Zamawiającym w sprawach związanych z przeprowadzeniem audytu, przekazaniem niezbędnych dokumentów i wizyty w centrum danych.
- 3. Audyt będzie obejmował następujące obszary tematyczne:
  - a. certyfikaty bezpieczeństwa posiadane przez centrum danych,
  - b. procedury związane z kontrolą dostępu do centrum danych,
  - c. systemy klimatyzacji centrum danych,
  - d. zasilanie centrum danych w tym agregaty prądotwórcze, systemy UPS, dostawy energii,
  - e. systemy gaśnicze,
  - f. systemy monitorowania warunków środowiskowych,

- g. zabezpieczenie łącza Internetowego,
  - h. dostawcy łącza internetowego,
  - i. procedury związane ze zgłaszaniem incydentów w centrum danych,
  - j. ochrona fizyczna centrum danych.
4. Audyt w centrum danych będzie przeprowadzany maksymalnie w czasie 2 godzin. Wykonawca powinien udostępnić zamawiającemu dokumenty związane z przeglądami systemów klimatyzacji, agregatów prądotwórczych, UPS, Systemów gaśniczych, monitorujących warunki środowiskowe.

#### **VIII. Wymagania związane z optymalizacją obciążenia serwerów**

1. Wykonawca będzie świadczył usługę optymalizacji obciążenia serwerów (load balancing) dla aplikacji webowej przy pomocy platformy sprzętowej składającej się z co najmniej dwóch urządzeń działających w klastrze wysokiej dostępności HA lub przy pomocy dedykowanego appliance.
2. Ze względu na bezpieczeństwo oraz na niezawodność pracy, Wykonawca nie dopuszcza rozwiązań typu Open Source.
3. Zamawiający dopuszcza możliwość współdzielenia urządzenia z innymi klientami Wykonawcy, pod warunkiem zapewnienia pełnej separacji od sieci innych klientów.
4. Pojedyncze urządzenie wchodzące w skład klastra, powinno spełniać następujące wymagania:
  - a. musi mieć możliwość zapewnienia minimum 1 Gbps przepustowości dla ruchu SSL
  - b. musi pozwalać na minimum 25 000 jednoczesnych połączeń TCP
  - c. powinno posiadać wydajność szyfrowania na poziomie 10000 nowych połączeń CPS SSL dla klucza RSA 2048 oraz P256 ECC SSL.
  - d. musi zapewniać możliwość rozkładania obciążenia za pomocą algorytmów minimum: Fastest Connection, Inbound/Outbound Bandwidth, Concurrent Connections.
  - e. musi zapewniać load balancing bazując na informacjach z warstw 4-7 modelu OSI ISO.
  - f. musi wspierać monitorowanie dostępności usług na serwerze za pomocą protokołów HTTP i HTTPS (aktywne próbkowanie).
  - g. powinno obsługiwać funkcje: websocets, sticky sessions, SSL Passthrough, terminację SSL, modyfikacje treści w warstwie ISO/OSI L7 (modyfikacja nagłówków HTTPS – np. X-Forwarded-For, X-Forwarded-Proto).