# Opis przedmiotu zamówienia

Świadczenie usługi kolokacji infrastruktury teleinformatycznej Zamawiającego w Data Center

|  |  |  |
| --- | --- | --- |
| Lokalizacja usługi | Parametr Wymagany (TAK) | Odpowiedź oferenta |
| Usługa kolokacji ma być realizowana w obiekcie typu Data Center zlokalizowanym **na terenie województwa śląskiego (Polska).** |  |  |
| Wykonawca wskaże w ofercie: |  |  |
| dokładny adres obiektu (miejscowość, ulica, nr budynku), |  |  |
| tytuł prawny do obiektu (własność, najem, operator), |  |  |
| podstawowe parametry obiektu (standard Data Center, dostęp 24/7/365, redundancja zasilania/chłodzenia). |  |  |
| Zakres świadczenia |  |  |
| Przedmiotem zamówienia jest kompleksowa usługa kolokacji obejmująca co najmniej: |  |  |
| **Szafę rack 42U** |  |  |
| * Szafa teleinformatyczna 19" o co najmniej wysokości 42U (jednostki rack), zamykana, przeznaczona do kolokacji, |  |  |
| * Wyłączne użytkowanie szafy przez Zamawiającego (dedykowana szafa, brak dzielenia z innymi klientami), |  |  |
| * Dostęp fizyczny do szafy przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku (24/7/365) w sposób stały, niezawodny i zgodny z procedurami bezpieczeństwa obiektu, |  |  |
| * Możliwość blokady szafy przez Zamawiającego (zgodnie z regulaminem obiektu), |  |  |
| * Prowadzenie okablowania wewnątrz szafy (organizery pion/poziom, przepusty kablowe, system zarządzania przewodami). |  |  |
| **Zasilanie – 5 kW** |  |  |
| * Wykonawca zapewni zasilanie dla urządzeń zainstalowanych w szafie o następujących parametrach: |  |  |
| * Moc dostępna: 5 kW łącznej mocy przyłączeniowej do dyspozycji Zamawiającego (ciągle dostępna, gwarantowana), |  |  |
| * Redundancja zasilania: co najmniej dwa niezależne tory zasilania (A/B) do szafy; dystrybucja mocy poprzez co najmniej dwie niezależne listwa PDU (Power Distribution Units) z pomiarami poboru energii (na poziomie PDU lub per gniazdo – do wskazania w ofercie), |  |  |
| * Gwarancja zasilania: zasilanie podstawowe z sieci elektroenergetycznej zabezpieczone systemem UPS (zasilacz awaryjny) oraz agregatem prądotwórczym z automatycznym przełączaniem w przypadku zaniku napięcia; system przełączania ma działać bez utraty zasilania (seamless), |  |  |
| * Zabezpieczenia: ochrona przeciwprzepięciowa i przeciwprzeładunkowa na wszystkich liniach zasilających szafę (odpowiedzialność Wykonawcy), |  |  |
| * Pomiary i monitorowanie: możliwość odczytania pomiarów poboru energii w szafie przez Zamawiającego (np. poprzez portal, API, e-mail z raportami) – do uzgodnienia w umowie, |  |  |
| * Model rozliczania: Wykonawca wskaże w ofercie, czy moc 5 kW jest rozliczana jako moc zarezerwowana (ryczałt bez względu na zużycie) czy jako limit średni/szczytowy – wybór modelu ma być jasny i uwzględniony w cenie brutto. |  |  |
| **Chłodzenie** |  |  |
| * Zapewnienie chłodzenia umożliwiającego bezpieczną, stabilną pracę urządzeń zainstalowanych w szafie przy obciążeniu cieplnym odpowiadającym 5 kW mocy IT, |  |  |
| * Utrzymanie warunków środowiskowych (temperatura i wilgotność) w standardzie obowiązującym dla profesjonalnych obiektów Data Center – Wykonawca poda w ofercie target parametry (np. temperatura 18–27°C, wilgotność 20–80% RH lub inne wymagane przez producenta sprzętu IT), |  |  |
| * Monitoring 24/7 warunków termicznych w obiekcie z procedurą alertowania w przypadku przekroczeń lub awarii systemu chłodzenia, |  |  |
| * Brak dodatkowych opłat za „in-row cooling" lub „cold aisle/hot aisle" (jeśli są stosowane w obiekcie) – albo wyszczególnienie ich w cenie ryczałtowej; wszelkie dodatkowe rozwiązania chłodzące muszą być wliczone w cenę brutto 36/60 miesięcy. |  |  |
| **Internet i adresacja IP** |  |  |
| * Łącze Internetowe symetryczne o przepustowości co najmniej 1 Gb/s (giga-bit na sekundę, dwukierunkowo), |  |  |
| * Publiczna adresacja IPv4: co najmniej pula /28 (16 adresów, z czego 14 użytecznych), routowana do infrastruktury Zamawiającego, |  |  |
| * Zakończenie łącza w szafie Zamawiającego poprzez port Ethernet 1 GbE (RJ-45) lub interfejs SFP/SFP+ (typ interfejsu Wykonawca wskaże w ofercie), |  |  |
| * Dostęp do łącza bez filtrów zawartości/web-filtrów (jeśli inaczej nie uzgodniono); w razie potrzeby ochrony DDoS – jako usługa dodatkowa do wyceny, |  |  |
| * Publiczna pula /28 routowana statycznie lub poprzez BGP (sposób routowania Wykonawca wskaże w ofercie oraz wyjaśni w dokumentacji technicznej), |  |  |
| * NOC/Service Desk dostępny 24/7 dla zgłaszania incydentów związanych z łączem. |  |  |
| * IPv6 (opcjonalnie, bez dodatkowych opłat): |  |  |
| * Zamawiający nie wymaga IPv6 jako warunku udziału w postępowaniu, jednak Wykonawca zobowiązany jest zapewnić możliwość uruchomienia IPv6 (prefiks /64 lub większy) w trakcie trwania umowy, bez dodatkowych opłat za uruchomienie i routowanie, |  |  |
| **Dostęp fizyczny 24/7/365** |  |  |
| * Zamawiający lub wskazane przez niego osoby mają prawo dostępu do obiektu i do urządzeń zainstalowanych w szafie przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, |  |  |
| * Dostęp regulowany procedurami bezpieczeństwa obiektu (autoryzacja, rejestr wejść, ewentualnie awizacja) – jednak procedury nie mogą ograniczać dostępności poniżej 24/7/365 dla osób upoważnionych przez Zamawiającego, |  |  |
| * Osób upoważnionych może być kilka; procedura upoważniania musi być szybka i nie wymagać zgody innej strony (wystarczy zawiadomienie o zmianie personelu), |  |  |
| * Możliwość bezpłatnego zmiany personelu dostępowego bez jakichkolwiek dodatkowych formalności lub opłat. |  |  |
| **Drugi ośrodek Data Center (wymóg dla rozbudowy)** |  |  |
| * Wykonawca musi dysponować (samodzielnie lub w ramach grupy kapitałowej, lub poprzez podwykonawcę wskazanego w ofercie) drugim, niezależnym ośrodkiem przetwarzania danych (Data Center, serwerownią), położonym w innej lokalizacji niż pierwszy ośrodek, |  |  |
| * Drugi ośrodek będzie dostępny do ewentualnego rozszerzenia usług Zamawiającego w przyszłości (kolokacja dodatkowych serwerów, redundancja, DR – disaster recovery), |  |  |
| * Na etapie składania oferty Wykonawca zobowiązany jest podać: |  |  |
| * + adres (miejscowość, województwo) drugiego DC, |  |  |
| * + krótką charakterystykę parametrów (dostęp 24/7/365, zasilanie/chłodzenie, dostępność łącz), |  |  |
| * + informację, czy możliwe są usługi łączności między ośrodkami (np. transmisja L2/L3, cross-connect, dedicated link) |  |  |
| **Wsparcie operacyjne i obsługa zgłoszeń** |  |  |
| * Wsparcie dostępne 24/7/365 dla zgłaszania incydentów krytycznych (zasilanie, chłodzenie, łącze), |  |  |
| * Kanały kontaktu: |  |  |
| * + Telefon |  |  |
| * + e-mail |  |  |
| * + ewentualnie system ticketowy (do uzgodnienia w umowie), |  |  |
| * Gwarantowane czasy reakcji: na incydenty krytyczne do 30 minut od momentu zgłoszenia (w trakcie pierwszego nawiązania kontaktu), |  |  |
| * Gwarantowany czas usunięcia awarii: do 4 godzin dla incydentów krytycznych (zasilanie/chłodzenie), do 8 godzin dla łącza (lub parametry wymagane przez Zamawiającego – do uzgodnienia), |  |  |
| * Raportowanie: dostępność usługi raportowana minimum raz w miesiącu (albo na żądanie) w postaci raportu z procentowym wskaźnikiem uptime dla zasilania/chłodzenia oraz łącza. |  |  |
| **Bezpieczeństwo fizyczne obiektu** |  |  |
| * Ochrona obiektu 24/7/365 (ochrona fizyczna, monitoring CCTV w częściach wspólnych), |  |  |
| * Kontrola dostępu (karta dostępu/biometria/PIN) z rejestracją wszystkich wejść i wyjść, |  |  |
| * Procedury bezpieczeństwa dla gości i pracowników zewnętrznych (z wymaganym zaawizowaniem), |  |  |
| * Strefowanie obiektu (oddzielenie pomieszczeń klientowskich od stref technicznych i magazynowych), |  |  |
| * Ochrona przed zagrożeniami fizycznymi: system przeciwpożarowy (detekcja dymu, systemy gaszące – niezagrażające sprzętowi IT), systemy oddymiające, wyjścia ewakuacyjne. |  |  |
| **Zgodność ze standardami i bezpieczeństwem informacji** |  |  |
| Wykonawca powinien dysponować lub wdrażać co najmniej: |  |  |
| * ISO/IEC 27001 (certyfikat) albo równoważne, udokumentowane procedury zarządzania bezpieczeństwem informacji obejmujące: kontrolę dostępu, identyfikację i uwierzytelnianie personelu, zarządzanie incydentami, procedury audytów wewnętrznych, |  |  |
| * Procedury ciągłości działania (Business Continuity/Disaster Recovery) udokumentowane i testowane regularnie (minimum raz w roku), |  |  |
| * Procedury reagowania na incydenty (Incident Response Plan) z czasami eskalacji i powiadamiania klientów, |  |  |
| * Jeśli Wykonawca nie posiada certyfikatu ISO/IEC 27001, zobowiązany jest dostarczyć dokumentację potwierdzającą zastosowanie ww. procedur i kontroli (certyfikat wewnętrzny, audyt niezależny, itp.). |  |  |
| **Okres świadczenia usługi** |  |  |
| Usługa kolokacji będzie świadczona przez: |  |  |
| Poniżej 36 miesięcy | 0 - punktów |  |
| Okres od 36 do 48 miesięcy | 10 - punktów |  |
| Okres od 49 do 60 miesięcy | 15 - punktów |  |
| 61 miesięcy i więcej | 20 - punktów |  |
| Równoważność w opisie przedmiotu zamówienia |  |  |
| Jeżeli powyższe wymagania wskazują normy, standardy, certyfikaty, technologie lub rozwiązania o określonych cechach (np. ISO/IEC 27001, szafa 19" 42U, Internet 1 Gb/s symetryczny), Zamawiający dopuszcza rozwiązania równoważne, o ile Wykonawca wykaże równoważność poprzez wskazanie, że rozwiązanie spełnia wszystkie kryteria funkcjonalne i jakościowe określone w OPZ. |  |  |
| Wymagania bezpieczeństwa informacji i procedur |  |  |
| **Zarządzanie dostępem** |  |  |
| * Kontrola dostępu do obiektu i szafy (autentykacja: karta, kod PIN, biometria), |  |  |
| * Rejestr wejść i wyjść z logowaniem czasowym, |  |  |
| * Procedura zmiany uprawnień dostępu dla personelu Zamawiającego, |  |  |
| * Możliwość czasowego zawieszenia dostępu (np. w okresie nieużytkowania szafy). |  |  |
| **Zarządzanie incydentami** |  |  |
| Wykonawca zobowiązany jest: |  |  |
| * Prowadzić rejestr incydentów bezpieczeństwa i infrastruktury, |  |  |
| * Powiadamiać Zamawiającego o wszelkich incydentach dotyczących usługi w ciągu 2 godzin od wykrycia, |  |  |
| **Zgodność z regulacjami** |  |  |
| Wykonawca zobowiązany jest do stosowania się do: |  |  |
| * Polskiego prawa (w tym RODO, Ustawy o ochronie konkurencji, Ustawy o podatku handlowym), |  |  |
| * Międzynarodowych standardów bezpieczeństwa (ISO/IEC 27001 lub równoważnych procedur), |  |  |
| * Procedur bezpieczeństwa wymaganego przez branżę (jeśli dotyczy). |  |  |
| Warunki specjalne i uwagi |  |  |
| **Dostęp dla autoryzowanych osób** |  |  |
| Zamawiający ma prawo do wyznaczenia kilku osób upoważnionych do wejścia do obiektu i do szafy. Procedura upoważniania musi być szybka i bezpłatna, bez konieczności osobistej autoryzacji ze strony Wykonawcy. |  |  |
| **Prawo do fotografowania i dokumentacji** |  |  |
| Zamawiający może fotografować i dokumentować stanu szafy i infrastruktury (dla celów audytowych/dokumentacji wewnętrznej); Wykonawca nie ma prawa do ograniczania tego prawa poza przypadkami zagrażającymi bezpieczeństwu obiektu. |  |  |
| **Prawo do migracji usług** |  |  |
| W przypadku rozwiązania umowy Zamawiający ma prawo do co najmniej 60 dni na demontaż i przeniesienie swoich urządzeń z szafy (bez dodatkowych opłat za utrzymanie szafy w tym okresie). |  |  |
| **Prawo do audytów** |  |  |
| Zamawiający zastrzega sobie prawo do przeprowadzenia audytów bezpieczeństwa i infrastruktury obiektu (w uzasadnionym terminie, z co najmniej 2-tygodniową awizacją) w celu weryfikacji zgodności z umową. |  |  |
| **Zamówienia dodatkowe** |  |  |
| Zamawiający wymaga informacji o możliwości: |  |  |
| * Kolokacji dodatkowych szaf/serwerów w tym samym obiekcie (ceny, dostępność), |  |  |
| * Kolokacji w drugim ośrodku (ceny, dostępność, czas wdrożenia), |  |  |
| * Usług łączności między ośrodkami (cross-connect, dedykowana transmisja). |  |  |