Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy: postępowania prowadzonego w trybie przetargu nieograniczonego pn. „Zapewnienie dostępu do Internetu na terenie Bazy Spółki, udostępnienie i pełna obsługa serwera internetowego, system do publikacji w Internecie stron podmiotowych BIP".

Znak sprawy: **KML-50/2023**

I. Przedmiot zamówienia

Przedmiot zamówienia winien być realizowany poprzez:

1. **Zapewnienie dostępu do sieci Internet.**

   1.1. Zapewnienie Zamawiającemu dostępu do sieci Internet poprzez łącze symetryczne o gwarantowanej przepustowości min. 100 Mbit/s.

   1.2. Zapewnienie Zamawiającemu stałej podsieci publicznych adresów IP – min. 16 adresów.

   1.3. Brak ograniczeń ilości przesyłanych danych.

   1.4. Do oferty winna być załączona informacja o typie zastosowanego łącza oraz typie, modelu i nazwie producenta urządzeń końcowych. W trakcie realizacji usługi dostawy Internetu Zamawiający dopuszcza, w uzasadnionych przypadkach, zmianę łącza oraz zmianę urządzeń końcowych z zastrzeżeniem, iż nie mogą mieć one gorszych parametrów niż zaoferowane na dzień składania ofert. Wyklucza się stosowanie urządzeń radiowych pracujących na częstotliwościach nielicencjonowanych.

2. **Udostępnienie urządzenia UTM oraz systemu do przechowywania i analizy logów.**

   2.1. Udostępnienie Zamawiającemu urządzenia UTM z wszelkimi licencjami i subskrypcjami niezbędnymi do realizacji następujących funkcjonalności:

   2.1.1. Routing i obsługa łączy WAN:

   - w zakresie routingu urządzenie powinno zapewniać obsługę: routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM,
   - urządzenie musi umożliwiać obsługę co najmniej dwóch łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

   2.1.2. Kontrolę dostępu – FireWall klasy Stateful Inspection:

   - polityka Firewall musi uwzględniać adresy IP użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń,
   - system musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT, translację jeden do jeden i jeden do wielu oraz dedykowany ALG (Application Level Gateway) dla protokołów SIP,

- w ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN,
- system Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
  - haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
  - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
  - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów np. RADIUS lub API.

2.1.3. Ochronę przed malware – antivirus (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS):

- silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach,
- system musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

2.1.4. Poufność transmisji danych – IPSec VPN oraz SSL VPN:

- system musi umożliwiać konfigurację połączeń typu IPSec VPN i w zakresie tej funkcji musi zapewniać:
  - wsparcie dla IKE v1 oraz v2,
  - obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM),
  - obsługę protokołu Diffie-Hellman grup 19 i 20,
  - wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE,
  - tworzenie połączeń typu Site-to-Site oraz Client-to-Site,
  - monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
  - możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,
  - obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth,
  - mechanizm „Split tunneling" dla połączeń Client-to-Site,
- system musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
  - pracę w trybie Portal – gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0,
  - pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

2.1.5. Ochronę przed atakami – Intrusion Prevention System:

- ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,
- system powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach,
- baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora,
- administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur,
- system musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS,
- mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies,
- wykrywanie i blokowanie komunikacji C&C do sieci botnet,

2.1.6. Kontrolę treści – Web Filter:

- moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne,
- w ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy,
- filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard,
- administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy adresów URL,
- system musi umożliwiać blokowanie pojawianie się niechcianych treści w wynikach wyszukiwarek takich jak Google oraz Yahoo,
- administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania,
- w ramach systemu musi istnieć możliwość określania, dla których kategorii url lub wskazanych url system nie będzie dokonywał inspekcji szyfrowanych pakietów,

2.1.7. Kontrolę pasma oraz ruchu QoS i Traffic shaping:

- system Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu,
- musi istnieć możliwość określania pasma dla poszczególnych aplikacji,
- system musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL,

2.1.8. Kontrolę aplikacji:

- funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP,

- baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora,
- aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików,
- baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P,
- administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur,

2.1.9. Zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention),

2.1.10. Analiza ruchu szyfrowanego protokołem SSL.

2.2. Urządzenie UTM musi posiadać nie mniej niż 16 portów Gigabit Ethernet RJ45.

2.3. Urządzenie UTM musi posiadać nie mniej niż 8 portów Gigabit Ethernet SFP.

2.4. Urządzenie UTM musi posiadać nie mniej niż 2 porty 10 Gigabit Ethernet SFP+.

2.5. Urządzenie UTM musi posiadać port konsoli szeregowej oraz port USB umożliwiający podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

2.6. Urządzenie UTM musi obsługiwać min. 1,5 mln jednoczesnych połączeń i min. 52 tys. nowych połączeń na sekundę.

2.7. Urządzenie UTM musi posiadać przepustowość Stateful Firewall: min. 18 Gbps dla pakietów 512 byte i min. 10 Gbps dla pakietów 64 byte.

2.8. Urządzenie UTM musi posiadać przepustowość Firewall min. 2,1 Gbps z włączoną funkcją kontroli aplikacji.

2.9. Urządzenie UTM musi posiadać wydajność szyfrowania VPN IPSec min. 10 Gbps.

2.10. Urządzenie UTM musi posiadać wydajność min. 1 Gbps w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu https.

2.11. Urządzenie UTM musi obsługiwać min. 2 tys. tuneli Gateway-to-Gateway IPsec VPN i min. 16 tys. tuneli Client-to-Gateway IPsec VPN.

2.12. Urządzenie UTM musi posiadać wydajność min. 1 Gbps dla skanowania ruchu enterprise mix z włączonymi funkcjami IPS, Application Control, Antivirus.

2.13. Urządzenie UTM musi posiadać możliwość definiowania w jednym urządzeniu nie mniej niż 10 wirtualnych firewall'i.

2.14. System do przechowywania i analizy logów musi współpracować z urządzeniem UTM.

2.15. System do przechowywania i analizy logów musi posiadać system dyskowy o pojemności min. 200 GB.

2.16. System do przechowywania i analizy logów musi umożliwiać zapis min. 1 GB logów na dzień.

2.17. System do przechowywania i analizy logów musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia UTM oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

- listę najczęściej wykrywanych ataków,

- listę najbardziej aktywnych użytkowników,
- listę najczęściej wykorzystywanych aplikacji,
- listę najczęściej odwiedzanych stron www,
- listę krajów, do których nawiązywane są połączenia,
- listę najczęściej wykorzystywanych polityk Firewall,
- informacje o realizowanych połączeniach IPSec.

2.18. System do przechowywania i analizy logów musi umożliwiać generowanie raportów w formatach PDF, HTML, CSV. Generowanie raportów musi odbywać się w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

2.19. System do przechowywania i analizy logów musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.

2.20. System do przechowywania i analizy logów musi zapewniać korelowanie zdarzeń co najmniej dla następujących kategorii zdarzeń: malware, aplikacje sieciowe, email, IPS, traffic, zdarzenia systemowe np. utracone połączenie vpn, utracone połączenie sieciowe.

2.21. System do przechowywania i analizy logów musi zapewniać konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

W przypadku awarii udostępnionego urządzenia UTM, Wykonawca zobowiązany jest do podstawienia urządzenia zastępczego w ciągu 4 godzin od zgłoszenia w dni robocze. Do oferty winna być załączona informacja o modelu i nazwie producenta urządzenia UTM i systemu do przechowywania i analizy logów. W trakcie realizacji usługi Zamawiający dopuszcza, w uzasadnionych przypadkach, zmianę urządzenia UTM z zastrzeżeniem, iż nie może mieć ono gorszych parametrów niż zaoferowane na dzień składania ofert.

3. Udostępnienie i obsługa serwera internetowego.

3.1. Udostępnienie Zamawiającemu wirtualnego serwera z zainstalowanym systemem Linux pełniącym funkcję serwera WWW, serwera poczty e-mail oraz serwera SFTP. Wirtualny serwer musi mieć przydzielone następujące zasoby infrastruktury serwerowej Wykonawcy: min. 8 rdzeni (core) procesora o częstotliwości min. 2.4 GHz, min. 16 GB RAM, min. 2 TB przestrzeni dyskowej.

3.2. Podłączenie ww. serwera do sieci Internet łączem symetrycznym o min. gwarantowanej przepustowości 100 Mbit/s.

3.3. Brak ograniczeń ilości przesyłanych danych do/z serwera.

3.4. Utrzymanie primary i secondary DNS dla domeny wod-kiel.com.pl.

3.5. Administrowanie ww. serwerem.

3.6. Zapewnienie codziennego backup'u ww. serwera.

3.7. Zapewnienie następujących funkcjonalności dla serwera:

3.7.1. Program do obsługi poczty przez WWW (połączenie szyfrowane).

3.7.2. Obsługa nielimitowanej ilości kont pocztowych.

3.7.3. Dowolna ilość aliasów pocztowych (dowolna-nazwa@wod-kiel.com.pl) do każdego konta.

3.7.4. Program do samodzielnego administrowania serwerem poczty e-mail poprzez WWW umożliwiający: samodzielne zakładanie kont pocztowych, samodzielną administrację aliasami pocztowymi, zmianę haseł dla konta pocztowego.

3.7.5. Zainstalowany serwer bazy danych MySQL.

3.7.6. Program administracyjny do nadzoru nad bazą MySQL.

3.7.7. Dostęp przez SFTP (możliwość samodzielnej aktualizacji serwisu WWW).

3.7.8. Obsługa PHP.

Wykonawca zobowiązany jest wykonać na własny koszt import wszystkich danych zgromadzonych przez Zamawiającego na obecnie używanym przez niego serwerze internetowym na swój serwer internetowy w ciągu 7 dni od daty podpisania umowy.

4. Udostępnienie systemu ochrony poczty email dla domeny wod-kiel.com.pl

4.1. System ochrony poczty musi realizować skanowanie antyspamowe i antywirusowe poczty przychodzącej i wychodzącej z wydajnością min. 1 tys. wiadomości/godzinę.

4.2. System ochrony poczty musi mieć możliwość tworzenia polityk filtrowania poczty w oparciu o adresy mailowe, nazwy domenowe, adresy IP.

4.3. System ochrony poczty musi posiadać możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.

4.4. System ochrony poczty musi posiadać funkcjonalność kwarantanny poczty z dziennym podsumowaniem dla użytkownika, z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.

4.5. System ochrony poczty musi posiadać białe i czarne listy adresów mailowych dla domen wskazanych przez administratora systemu.

4.6. System ochrony poczty musi posiadać białe i czarne listy adresów mailowych dla poszczególnych użytkowników.

4.7. W zakresie kontroli antywirusowej i ochrony przed malware udostępniony system ochrony poczty musi zapewniać:

4.7.1. Skanowanie antywirusowe wiadomości SMTP.

4.7.2. Skanowanie załączników skompresowanych.

4.7.3. Blokowanie załączników w oparciu o typ pliku.

4.7.4. Możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.

4.7.5. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości,

dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera.

4.8. W zakresie kontroli antyspamowej udostępniony system ochrony poczty musi zapewniać:

4.8.1. Reputację adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta systemu ochrony poczty.

4.8.2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta systemu ochrony poczty.

4.8.3. Szczegółową kontrolę nagłówka wiadomości.

4.8.4. Analizę Heurystyczną.

4.8.5. Współpracę z zewnętrznymi serwerami RBL, SURBL.

4.8.6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.

4.8.7. Możliwość dostrajania filtrów Bayes'a przez poszczególnych użytkowników.

4.8.8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.

4.8.9. Kontrolę w oparciu o Greylisting oraz SPF.

4.8.10. Filtrowanie treści wiadomości i załączników.

4.8.11. Kwarantannę zarówno użytkowników jak i systemową z możliwością edycji nagłówków wiadomości.

4.8.12. Ochronę typu outbrake.

4.8.13. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).

4.8.14. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodawanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera.

4.9. W zakresie ochrony przed atakami na usługę poczty udostępniony system ochrony poczty musi zapewniać:

4.9.1. Ochronę przed atakami na adres odbiorcy.

4.9.2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.

4.9.3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.

4.9.4. Kontrolę Reverse DNS (ochrona przed Anty-Spoofing).

4.9.5. Weryfikację poprawności adresu e-mail nadawcy.

5. Udostępnienie i obsługa podmiotowej strony Zamawiającego w ramach Biuletynu Zamówień Publicznych.

5.1. Udostępnienie i obsługa podmiotowej strony Zamawiającego w ramach Biuletynu Zamówień Publicznych wraz z wszelkimi licencjami niezbędnymi do wykorzystania oferowanego serwisu BIP u Zamawiającego. Rejestracja, obsługa i utrzymanie domeny na serwerze WWW Wykonawcy. Zainstalowanie systemu na komputerach Zamawiającego i przeszkolenie pracowników w siedzibie Zamawiającego.

5.2. Oferowany system musi spełniać wszystkie wymagania stawiane takim systemom przez akty prawne regulujące dostęp do informacji publicznej (Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej Dz. U. z 2019 poz. 1429 z późniejszymi zmianami, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej Dz. U. z 2007 r. nr 10 poz. 68).

5.3. Strona musi być zgodna ze standardem WCAG 2.1 na poziomie co najmniej AA dla systemów teleinformatycznych w zakresie dostępności dla osób niepełnosprawnych zgodnie z Ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. poz. 848), w tym w szczególności opracowanie szaty graficznej strony w wersji dla osób niedowidzących oraz przetwarzanie tekstu na mowę i odczytywanie treści strony na głos.

5.4. Serwis musi zawierać komunikat o korzystaniu z plików „Cookie" wraz z przyciskami „polityka prywatności" i „zgadzam się". Treść komunikatu oraz link otwierany po kliknięciu w przycisk „polityka prywatności" określa administrator w CMS. Przycisk „zgadzam się" ukrywa komunikat i zapisuje informację, że użytkownik zapoznał się z jego treścią (komunikat nie pojawia się do czasu usunięcia lub wygaśnięcia tej informacji).

5.5. Dostępność strony dla osób z niepełnosprawnością. Wykonawca musi opracować warstwę prezentacyjną aplikacji uwzględniającą wymagania WCAG 2.1 na poziomie AA. Wszystkie elementy HTML „A" muszą zawierać poprawnie wypełniony atrybut „TITLE", a elementy „IMG" muszą posiadać poprawnie wypełniony atrybut „ALT". Aplikacja musi pozwalać na przypisywanie atrybutu „TITLE" i „ALT" do wstawianych w edytorze elementów „A" i „IMG".

5.6. Strona musi być zoptymalizowana pod kątem czasu ładowania (mała łączna wielkość plików tworzących pojedynczą stronę).

5.7. Kodowanie strony zgodne ze standardami W3C: HTML 5, CSS 3 oraz WCAG 2.1. Strona musi przechodzić poprawnie walidacje zgodności z powyższymi standardami przy pomocy narzędzi udostępnionych przez W3C (HTML5: http://validator.w3.org/, CSS3: http://jigsaw.w3.org/css-validator/) oraz pod kątem wdrożenia WCAG 2.0 (np. www.achecker.ca).

5.8. Kody HTML szablonów graficznych powinny wyświetlać się prawidłowo na co najmniej następujących przeglądarkach internetowych: Edge, Chrome, Firefox, Safari, Opera dla oficjalnych najnowszych wersji produktów (tzw. wersji stabilnych) wydawanych przez producentów oraz dla trzech wersji wcześniejszych produktu, jak również dla przeglądarek tabletów i telefonów komórkowych instalowanych na najpopularniejszych urządzeniach mobilnych (tablety i telefony z systemem Android, iOS).

5.9. Wykonawca jest zobowiązany do dokonywania na bieżąco wszystkich zmian w oferowanym systemie, w celu dostosowywania go do obowiązujących w danym momencie przepisów prawnych w zakresie BIP, w terminie poprzedzającym wejście ich w życie.

5.10. Adres podmiotowej strony BIP: bip.wod-kiel.com.pl

Wykonawca zobowiązany jest wykonać na własny koszt import danych z obecnie używanego przez Zamawiającego systemu BIP do swojego systemu BIP (z zachowaniem obowiązujących przepisów prawnych) w ciągu 7 dni od daty podpisania umowy.

II. Istotne informacje dotyczące realizacji zamówienia

1. **Wykonawca jest zobowiązany załączyć do oferty informację o typie zastosowanego łącza oraz typie, modelu i nazwie producenta urządzeń końcowych w punkcie 4 ppkt 5) Formularza oferty stanowiącego Załącznik nr 2. W trakcie realizacji przedmiotu zamówienia Zamawiający dopuszcza, w uzasadnionych przypadkach, zmianę łącza oraz zmianę urządzeń końcowych z zastrzeżeniem, iż nie mogą być one gorsze niż zaoferowane na dzień składania ofert. Wyklucza się stosowanie urządzeń radiowych pracujących na częstotliwościach nielicencjonowanych.**

III. Warunki udziału w postępowaniu

1. Wymagane jest, aby Wykonawca zapewniający dostęp do sieci Internet na terenie Bazy Spółki był wpisany do rejestru przedsiębiorstw telekomunikacyjnych, prowadzonych przez Prezesa Urzędu Komunikacji Elektronicznej, zgodnie z art. 10 ust. 1 *Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* (tekst jednolity Dz. U. 2021 poz. 576 z późniejszymi zmianami) oraz *Ustawie z dnia 6 marca 2018 roku Prawo przedsiębiorców* (art. 43 dot. rejestrów działalności regulowanej).

   W celu potwierdzenia spełnienia ww. warunku Zamawiający wymaga, aby Wykonawca dołączył na wezwanie Zamawiającego Oświadczenie stanowiące Załącznik nr 8 potwierdzające wpis do rejestru przedsiębiorstw telekomunikacyjnych, prowadzony przez Prezesa Urzędu Komunikacji Elektronicznej (kopia potwierdzona za zgodność z oryginałem).

2. Zamawiający dopuszcza podzlecenie wykonania przedmiotu zamówienia podwykonawcy, pod warunkiem, iż jest on wpisany do rejestru przedsiębiorstw telekomunikacyjnych, prowadzonych przez Prezesa Urzędu Komunikacji Elektronicznej, zgodnie z art. 10 ust. 1 *Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* (tekst jednolity Dz. U. 2021 poz. 576 z późniejszymi zmianami) oraz *Ustawie z dnia 6 marca 2018 roku Prawo przedsiębiorców* (art. 43 dot. rejestrów działalności regulowanej).

   W celu potwierdzenia spełnienia ww. warunku należy dołączyć na wezwanie Zamawiającego Oświadczenie stanowiące Załącznik nr 8 potwierdzające wpis do rejestru przedsiębiorstw telekomunikacyjnych (kopia potwierdzona za zgodność z oryginałem) dla każdego z podwykonawców.

IV. Pozostałe warunki postępowania

1. Nie dopuszcza się możliwości składania ofert częściowych.
2. Nie dopuszcza się możliwości składania ofert wariantowych.
3. Nie dopuszcza się rozliczania zamówienia w walutach innych niż polski złoty.