Fundusze Europejskie Infrastruktura i Środowisko | Rzeczpospolita Polska | Ministerstwo Zdrowia | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Chojnice, dnia 23.06.2023 r

Zapytanie ofertowe nr

1/e-POZ/2023

Na zakup sprzętu teleinformatycznego w celu rozbudowy systemu gabinetowego Placówki POZ dla

potrzeb wdrożenia procesów biznesowych oraz umożliwienia świadczenia e-usług publicznych realizowany w ramach projektu *„Wdrożenie e-Usług w Placówce POZ*", nr POIS.11.03.00-00-0074/22,

współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Infrastruktura i Środowisko na lata 2014-2020 na podstawie umowy nr UM.POZ2.U-10831.2022-00/4536/2023/275 o powierzenie Grantu na realizację przedsięwzięcia.

KOD CPV 32420000-3 - Urządzenia sieciowe

KOD CPV 32413100-2 - routery sieciowe

ZAMAWIAJĄCY:
SAMODZIELNA PUBLICZNA PRZYCHODNIA WIEJSKA GMINY CHOJNICE,
ul. KOŚCIERSKA 9, 89-600 CHOJNICE
NIP: 5551783986, REGON: 090103299

1. **Opis przedmiotu zamówienia:**

Przedmiotem zamówienia jest dostawa elementów infrastruktury teleinformatycznej wskazanych w pkt II.1 i II.2 Modelu referencyjnego, niezbędnych dla rozbudowy lokalnych Aplikacji Gabinetowych oraz integracji z centralnym systemem e-zdrowia, w ramach przedsięwzięcia pn. Wdrożenie e-Usług w Placówce POZ.
Źródło finansowania: Program Operacyjny Infrastruktura i Środowisko 2014-2020, oś XI: REACT-EU, działanie: 11.3 Wspieranie naprawy i odporności systemu ochrony zdrowia, POIS.11.03.00-00-0074/22.

Celem zamówienia w zakresie zadania nr 1 jest:

Wdrożenie ZTNA (Zero Trust Network Access) wraz z MFA (Multi Factor Autentication) dla dostępów serwerowych - zapora sieciowa z wbudowanym IPS, systemem antywirusowym, url filterig, sandbox na poziomie firewalli i urządzeń końcowych.

Zakup urządzeń i oprogramowania:

2x FGT-100F w układzie klastra – licencja UTP Hardware plus 3 Year 24x7 FortiCare and FortiGuard Unified Threat Protection (UTP) wraz z oprogramowaniem Forticlient EPP/APT (On Pemise Deployments) 3 Year FortiClient EPP/APT Subscription for 75 endpoints, Includes VPN/ZTNA Agent, EPP/APT, on-prem EMS with 24x7 FortiCare., FortiAuthenticator [L]VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machin, VM License 3 Year 24x7 FortiCare Contract (1 - 500 USERS) System musi być zarządzany centralnie za pomocą FortiManagera, oraz zawierać system zarządzania tożsamością użytkowników FortiAuthenticator dla 100 użytkowniów

6x FG-40F ze wsparciem 3 Year FortiCare Essential Support wraz z agregacją linków

Okres pełnego wsparcia produktów: sprzętowego i programowego minimum 3 lata

Jednocześnie zestaw musi spełniać poniższe parametry wydajnościowe - dopuszcza się zastosowanie wyższych modeli Fortinetu, które będą spełniały następujące minimalne wymagania wydajnościowe:

Założenia projektowe:

Celem projektu jest modernizacja istniejącej infrastruktury opartej o urządzenia i oprogramowanie 2x Fortigate 50E w centrali i 6x Fortigate 30E po jednym w filiach, które mają zastać rozbudowane lub zastąpione nowoczesną siecią zapewniającą wdrożenie zaawansowanych funkcjonalności bezpieczeństwa (antywirus, url filtering, IPS, sandbox) na poziomie firewali oraz urządzeń końcowych oraz wdrożenie ZTNA wraz z MFA dla dostępu do zasobów serwerowych. Istniejąca redundantna infrastruktura AD ma być wykorzystana do uwierzytelniania w ZTNA.

Pomiędzy lokalizacjami zostaną skonfigurowane inteligentne połączenia SD-WAN. Firewall w Centrali czy jednostce zdalnej, będzie mógł dynamicznie wybierać wykorzystywane łącze na podstawie zdefiniowanych parametrów – np. jakość łącza w danym czasie. Mechanizmy bezpieczeństwa połączone z SD-WAN (w czterech lokalizacjach połączonych na łączach głównych i zapasowych z wykorzystanie przepływności obu łączy oraz z sygnalizacją uszkodzenia jednego z łączy) pozwalają w pełni kontrolować komunikację w obrębie sieci prywatnej oraz zabezpieczają dodatkowo ruch sieciowy do systemów w chmurze publicznej (platforma wyposażona jest w rozbudowany zestaw konektorów do integracji z różnymi środowiskami chmurowymi) jak również standardową komunikację użytkowników do sieci publicznej. Tu administrator decyduje w jaki sposób wykorzystywane będą łącza (w oparciu o elastyczne reguły), jak weryfikowana będzie jakość poszczególnych łączy, jak usługi i aplikacje będą priorytetyzowane i zabezpieczane. W efekcie, tworzone są zasady kontroli dostępu z zachowaniem mechanizmów kontroli stanu sesji, w których elementem, na podstawie którego podejmowana jest decyzja, jest zdefiniowany obiekt typu interfejs WAN. Jako parametry, którymi weryfikowane będą poszczególne łącza wchodzące w skład SD-WAN mogą być zastosowane: ping, TCP Echo, UDP Echo, HTTP, TWAMP, ale również parametry takie jak: opóźnienie, zmienność opóźnienia, straty pakietów.

Wykorzystanie mechanizmów SD-WAN określa się w elastycznych regułach, w których decyzje podejmowane są w oparciu o:

a. Użytkowników, Grupy użytkowników.
b. Aplikacje sieciowe i chmurowe (baza ISDB aktualizowana przez producenta).
c. Adresy źródłowe i docelowe.
d. Wymagane parametry łącza.

Każde urządzenie ma podejmować decyzje dotyczące obsługi ruchu autonomicznie

Wymagane są następujące funkcjonalności urządzeń (oprogramowania) tego typu w układzie klastra dla jednostki centralnej połączonej likami zagregowanymi do istniejącego stacka switchy:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – urządzenia zestawić w klaster Active-Active i Active-Passive po ustaleniu z zamawiającym. W obu trybach ma istnieć funkcja synchronizacji sesji firewall;
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych;
3. Monitoring stanu realizowanych połączeń VPN;
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Musi istnieć możliwość tworzenia interfejsów redundantnych, wdrożyć łącznie minimum osiem interfejsów redundantnych z agregacją linów;
5. System realizujący funkcję Firewall musi dysponować interfejsami dla jednostek centralnych:
   a. Gigabit Ethernet RJ-45;
   b. SFP 1 Gbps;

Dla jednostek zdalnych Gigab*it Ethernet RJ-45;*

6. System Firewall musi posiadać wbudowany port konsolowy oraz gniazdo USB oraz instalacji oprogramowania z klucza USB;
7. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q;
8. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową, która zapewni przetrzymywanie logów i ruchu sieciowego co najmniej 3 miesiące wstecz (ruch sieciowy) oraz 12 miesięcy wstecz (logi systemu);
9. W zakresie Firewall 'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę ;
10. Przepustowość Stateful Firewall: nie mniej niż **20 Gbps** dla pakietów 512 B ;
11. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji IPS: nie mniej niż 1.6 Gbps dla jednostek centralnych i 0,8 Gbps dla jednostek zdalnych
12. Wydajność szyfrowania IPSec VPN nie mniej niż 2.6 Gbps, wydajność Threat Protection minimum 1Gbps dla jednostek centralnych i odpowiednio IPS 1Gbps i Threat Protection 0,6 Gbps dla jednostek zdalnych
13. Wydajność skanowania ruchu w celu ochrony przed atakami z zewnątrz i wewnątrz (ochrona IPS) minimum **5 Gbps**;
14. Wydajność skanowania z włączonymi funkcjami: IPS, Application Control, Antywirus, Web Filter minimum **3 Gbps**;
15. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu https minimum **4 Gbps**;
16. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:
    a. Ochrona IPS;
    b. Dostosowanie aktualnej antywirusowej/malware w opraciu o istniejące oprogramowanie ESET co najmniej dla protokołów SMTP, SMTPS, POP3, IMAP, IMAPS, HTTP, HTTPS, FTP;
    c. Kontrola Aplikacji;

d. Kontrola stron WWW;
e. Kontrola zawartości poczty (ochrona przed spamem);
f. Ochrona przed sieciami botnet;
g. Kontrola zapytań DNS;
h. Deszyfracja SSL (Inspekcja ruchu szyfrowanego);
i. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN;
j. Zarządzanie pasmem (QoS, Traffic shaping);

17. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP);
18. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site;
19. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2;
20. Analiza ruchu szyfrowanego protokołem SSH;
21. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z funkcją filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system;
22. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń i rejestrowanie zdarzeń;
23. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    a. Translację jeden do jeden oraz jeden do wielu;
    b. Dedykowany ALG (Application-Level Gateway) dla protokołu SIP;
24. W ramach systemu musi zapewniać tworzenie wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN;
25. Zapewnia wykorzystanie w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików;
26. System zapewnia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    a. Wsparcie dla IKE v1 oraz v2;
    b. Obsługa szyfrowania protokołem minimum AES z kluczem 128 i 256 bitów;
    c. Obsługa protokołu Diffie-Hellman minimum grup 19 i 20;
    d. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site;
    e. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności;
    f. Wybór tunelu przez protokoły minimum : dynamicznego routingu (np. OSPF) oraz routingu statycznego;
    g. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth;
    h. Mechanizm „Split tunneling” dla połączeń Client-to-Site;
27. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    a. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki;
    b. Pracę w trybie tunnel z funkcjonalnością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta;
    c. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN;
28. W zakresie routingu rozwiązanie powinno zapewniać minimum obsługę:
    a. Routingu statycznego;
    b. Policy Based Routingu;
    c. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM;
29. System ma wykorzystywać protokoły dynamicznego routingu przy konfiguracji

równoważenia obciążenia do łączy WAN;
30. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu;
31. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu;
32. Musi istnieć funkcjonalność określania pasma dla poszczególnych aplikacji;
33. System zapewnia zarządzanie pasmem dla wybranych kategorii URL;
34. Silnik antywirusowy zapewnia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021);
35. System zapewnia skanowanie archiwów, w tym co najmniej: zip, rar;
36. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze;
37. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office;
38. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych;
39. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach;
40. Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;
41. Administrator systemu ma zapewnione definiowanie własnych wyjątków oraz własnych sygnatur;
42. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS;
43. System zapewnia mechanizmy ochrony dla aplikacji Webowych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz kontrolowanie długości nagłówka, ilości parametrów URL, Cookies;
44. Wykrywanie i blokowanie komunikacji C&C do sieci botnet;
45. Funkcja Kontroli Aplikacji zapewnia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP;
46. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików;
47. Baza musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P;
48. Administrator systemu ma zapewnione definiowanie wyjątków oraz własnych sygnatur;
49. 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;
50. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard;
51. Administrator otrzymuje do dyspozycji funkcję nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL;
52. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo;
53. Administrator otrzymuje do dyspozycji funkcję definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania;
54. W ramach systemu dostarczona jest funkcja określająca, dla których kategorii url lub wskazanych url, system nie będzie dokonywał deszyfracji SSL w komunikacji;
55. System Firewall musi posiadać weryfikację tożsamości użytkowników minimum za pomocą;
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu;
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP;
    c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych;
    d. Musi być dostępna funkcja zastosowania w tym procesie uwierzytelniania dwuskładnikowego;

56. Rozwiązanie zapewnia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API;
57. Elementy systemu bezpieczeństwa muszą być zarządzane lokalnie z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania;
58. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów;
59. System zapewnia włączenie mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego;
60. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow;
61. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall;
62. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej;
63. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona funkcja jednoczesnego wysyłania logów do wielu serwerów logowania;
64. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu;
65. System musi zapewniać logowanie do serwera SYSLOG;
66. W komplecie z urządzeniem muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres nie krótszy niż 36 miesięcy;
67. System musi być zarządzany centralnie poprzez FortiManager
68. System musi mieć wieloskładnikowe uwierzytelnianie MFA
69. System zarządzania tożsamością użytkowników za pomocą FortiAuthenticator 100 users
70. Jednocześnie wydajność urządzeń i oprogramowania musi zapewnić następujący wzrost obciążenia związany z rozwojem przepływności łączy:

Opis	Parametry obecne	Parametry planowane
Liczba filii	6	6
Prędkość transmisji intranetu	50Mbit/s – symetryczne	300Mbit/s symetryczne
Prędkość transmisji z internetem filie	download 15Mbits/s, upload 5Mbit/s	download 300Mbit/s, upload 50Mbit/s
Prędkość transmisji z internetem centrala	download 150Mbit/s, upload 50Mbit/s	download 1000Mbit/s, upload 500Mbit/s
Prędkość LAN	1Gbit/s	10Gbit/s
Prędkość LAN – serwery lokalne	10Gbit/s	40Gbit/s

71. Ruch z filii ma być kierowany do Internetu i z Internetu przez przychodnię centralną w oparciu o dostarczone rozwiązanie sprzętowe i programowe w układzie klastra (active/passive). Firewalle podłączyć linkami zagregowanymi do stacka switchy w obecnie istniejącej w infrastrukturze.
72. Okres pełnego wsparcia sprzętowego i programowego minimum 3 lata.
73. Firewalle muszą być wyposażone w pakiet licencji UTP
74. Termin instalacji i kompletnego wdrożenia 14 sierpnia 2023

We wszystkich przypadkach, w których ze względu na specyfikację przedmiotu zamówienia wskazano pochodzenie, nazwy materiałów, urządzeń, oprogramowanie, systemy lub ich pochodzenie dopuszcza się stosowanie materiałów, urządzeń, systemy równoważne, tj. wszelkie wymienione z nazwy materiały, urządzenia, systemy użyte w przekazanej przez Zamawiającego dokumentacji lub ich pochodzenie, służą

wyłącznie określeniu standardu i mogą być zastąpione innymi o nie gorszych parametrach technicznych, użytkowych, jakościowych, funkcjonalnych i walorach estetycznych przy uwzględnieniu prawidłowej współpracy z pozostałymi materiałami, urządzeniami.

Ewentualne wskazane nazwy produktów oraz ich producentów nie mają na celu naruszenia zasady uczciwej konkurencji i równego traktowania wykonawców. Pojęcie równoważności znajduje również zastosowanie w przypadku, gdy Zamawiający opisał przedmiot zamówienia za pomocą norm, aprobat, specyfikacji technicznych i systemów odniesienia.

Ewentualne zamieszczone w dokumentach nazwy producentów użyto jedynie w celu przykładowym. Wszędzie gdzie są one wskazane należy czytać w ten sposób, że towarzyszy im określenie „lub równoważne". Przez pojęcie „lub równoważne" Zamawiający rozumie oferowanie materiałów zapewniających uzyskanie parametrów technicznych nie gorszych od założonych w ww. dokumentach. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia, ani do podwyższenia ceny, ani do naruszenia przepisów prawa.

W przypadku spełnienia powyższych warunków Zamawiający dopuszcza stosowanie rozwiązań równoważnych. W przypadku, gdy wykonawca zaproponuje asortyment równoważny, zobowiązany jest wykonać i załączyć do oferty zestawienie wszystkich zaproponowanych pozycji równoważnych i wykazać ich równoważność w stosunku do opisanych w dokumentacji, stanowiącej opis przedmiotu zamówienia, ze wskazaniem nazwy, strony i pozycji opisu przedmiotu zamówienia, których dotyczy. Jednocześnie Zamawiający informuje, że ciężar dowodu wykonania równoważności spoczywa na Wykonawcy.

Wszelkie koszty związane z dostarczeniem przedmiotu zamówienia ponosi wykonawca.

1.1. Wykonawca oświadczy, że wszystkie koszty wytworzenia przedmiotu Zamówienia, w tym koszty niezbędnego przeszkolenia pracownika Zamawiającego, zostały uwzględnione w oferowanej cenie.
1.2. Wykonawcy nie przysługuje prawo do ubiegania się o zapłatę jakichkolwiek kosztów dodatkowych, chyba że Strony zgodnie postanowią inaczej.
1.3. Wykonawca udzieli Zamawiającemu gwarancji zgodnie ze specyfikacją techniczną, liczonej od dnia Odbioru Końcowego.
1.4. Gwarancja obejmie zobowiązanie do usunięcia wszystkich zgłoszonych w okresie obowiązywania gwarancji usterek, w terminie nie późniejszym niż 14 dni roboczych od daty zgłoszenia, chyba że obiektywne, istotne okoliczności techniczne na to nie pozwolą.
1.5. Oferowany sprzęt musi być fabrycznie nowy (bez śladów użytkowania), kompletny, nieużywany, sprawny, wolny od wad materiałowych i konstrukcyjnych oraz nie może być przedmiotem praw ani zobowiązań osób trzecich.

2. **Termin realizacji i miejsce dostawy:**
   2.1. Termin realizacji zamówienia Zadania nr 1 do 14.08.2023r.,
   2.2. Adres dostawy: SAMODZIELNA PUBLICZNA PRZYCHODNIA WIEJSKA GMINY CHOJNICE , 89-600 Chojnice, ul. Kościerska 9.

3. **Warunki udziału w postępowaniu**
   3.1. Od Wykonawcy oczekuje się spełnienia następujących warunków udziału w postępowaniu.

3.1.1. Wykonawca posiada uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień.

3.1.2. Wykonawca zapewni wszystkie materiały i urządzenia niezbędne do realizacji zamówienia.

3.1.3. Wykonawca posiada niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania zamówienia.

3.1.4. Wykonawca zapewni do realizacji projektu minimum 1 specjalistę posiadającego doświadczenie w zakresie realizacji tego typu zamówienia.

3.1.5. Wykonawca znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

3.1.6. Wykonawca nie zalega z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne.

3.1.7. Wykonawca będący osobą fizyczną nie został prawomocnie skazany za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych.

3.1.8. Wspólnik spółki jawnej, partner lub członek zarządu spółki partnerskiej; komplementariusz spółki komandytowej oraz spółki komandytowo-akcyjnej; członek organu zarządzającego osoby prawnej nie został prawomocnie skazany za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych.

3.1.9. Sąd nie orzekł wobec wykonawcy zakazu ubiegania się o zamówienia, na podstawie przepisów o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary.

3.2. Weryfikacja spełnienia warunków udziału w postępowaniu odbędzie się w oparciu o oświadczenia i dokumenty załączone do oferty – według wzorów zawartych w załączniku nr 1 do niniejszego zapytania ofertowego.

4. **Warunki wykluczenia**

4.1. Zamawiający nie może udzielić zamówienia podmiotowi powiązanemu z nim osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu zamawiającego lub osobami wykonującymi w imieniu zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

4.1.1. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;

4.1.2. posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez IZ PO;

4.1.3. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;

4.1.4. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli.

4.2. Zamawiający nie może udzielić zamówienia osobom i podmiotom, które podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).

4.3. Wymogiem formalnym jest dołączenie podpisanego oświadczenia – według wzoru zawartego w załączniku nr 1 do niniejszego postępowania.

5. **Termin i formy składania oferty**

5.1. Oferty należy składać na załączonym formularzu (Załącznik nr 1) do dnia 03.07.2023r. do godziny 09:00 wyłącznie w jeden z poniższych sposobów:

5.1.1. pocztową przesyłką rejestrowaną albo kurierem na adres zamawiającego: SAMODZIELNA PUBLICZNA PRZYCHODNIA WIEJSKA GMINY CHOJNICE, ul. KOŚCIERSKA 9, 89-600 CHOJNICE, NIP: 5551783986, REGON: 090103299

5.1.2. osobiście w siedzibie zamawiającego pod adresem: SAMODZIELNA PUBLICZNA PRZYCHODNIA WIEJSKA GMINY CHOJNICE, ul. KOŚCIERSKA 9, 89-600 CHOJNICE, NIP: 5551783986, REGON: 090103299, w godzinach 7^{00}-11^{00}, w gabinecie 022;

5.1.3. pocztą elektroniczną na adres: informatyk1@przychodniawiejska.pl w postaci skanu oferty wraz z wymaganymi załącznikami. Oferta składana w postaci elektronicznej powinna zostać zeskanowana wraz ze wszystkimi załącznikami do jednego pliku w formacie PDF.

5.2. O terminie złożenia decyduje faktyczna data i godzina wpływu oferty do biura Zamawiającego, przy czym termin wpływu oferty zostanie zachowany w przypadku wpływu wersji elektronicznej oferty na adres e-mail.

6. **Sposób przygotowania oferty**

6.1. Oferta musi zostać złożona na formularzu stanowiącym załącznik nr 1 do niniejszego zapytania.

6.2. Oferta powinna być sporządzona w języku polskim oraz podpisana przez osobę upoważnioną do reprezentowania Wykonawcy.

6.3. Do oferty należy załączyć i trwale z nią zespolić:

6.3.1. sporządzone według wzoru załączonego do formularza oferty oświadczenie wykonawcy o spełnianiu warunków udziału w postępowaniu opisanych w punkcie 3;

6.3.2. sporządzone według wzoru załączonego do formularza oferty oświadczenie wykonawcy, że nie występują uniemożliwiające udzielenie zamówienia wykluczenia opisane w punkcie 4;

6.3.3. kopię aktualnego dokumentu rejestrowego (chyba, że jest on dostępny w ogólnodostępnych bazach), potwierdzający upoważnienie osoby podpisującej ofertę do reprezentowania Wykonawcy; jeśli upoważnienie do reprezentowania wykonawcy nie wynika z dokumentu rejestrowego, należy dołączyć pełnomocnictwo dla osoby podpisującej ofertę w imieniu wykonawcy.

6.4. Przez trwałe zespolenie rozumie się, iż:

6.4.1. w przypadku oferty składanej w wersji papierowej oferta wraz z wszystkimi załącznikami musi być zbindowana lub spięta zszywaczem;

6.4.2. w przypadku oferty składanej w wersji elektronicznej (za pośrednictwem e-mail) oferta wraz ze wszystkimi załącznikami musi być zeskanowana do jednego pliku w formacie pdf i podpisana.

6.5. Każdy Wykonawca może złożyć wyłącznie jedną ofertę, w której musi być zaoferowana tylko jedna cena za realizację Zadania nr 1.

6.6. Cena oferty musi być określona w złotych polskich (PLN), z dokładnością do dwóch miejsc po przecinku.

6.7. Jeśli zamawiający stwierdzi, iż załączone do oferty dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez zamawiającego wątpliwości, może wezwać wykonawcę do ich złożenia,

uzupełnienia lub poprawienia lub do udzielania wyjaśnień w formie i terminie przez siebie wskazanym.

6.8. Wykonawca, który nie załączy wszystkich wymaganych dokumentów zostanie wykluczony z postępowania o udzielenie zamówienia, a jego oferta zostanie odrzucona.

7. **Termin związania ofertą**

Termin związania z ofertą wynosi 30 dni od daty złożenia oferty, przy czym Wykonawca samodzielnie lub na wniosek zamawiającego może przedłużyć termin związania ofertą, z tym że zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 30 dni.

8. **Kryteria oceny ofert:**

8.1. Za najkorzystniejszą uznana zostanie oferta, która uzyska największą liczbę punktów przyznanych w kryterium „Cena brutto".

8.2. Oferowana cena brutto za wykonanie zamówienia – waga 100%

Obliczenie oceny oferty w ramach kryterium „Oferowana cena brutto za wykonanie zamówienia" nastąpi wg następującego wzoru:

$$\text{Liczba punktów oferty} = \frac{\text{cena oferty najniższej}}{\text{cena oferty ocenianej}} \times 100$$

W ramach kryterium Wykonawca może otrzymać maksymalnie 100 punktów.

8.3. Za najkorzystniejszą uznana zostanie oferta, która uzyska największą liczbę punktów.

8.4. W przypadku braku możliwości rozstrzygnięcia z powodu otrzymania kilku ofert z identyczną liczbą punktów w danym Zadaniu, Zamawiający zaprosi oferentów, którzy uzyskali identyczną liczbę punktów, do ponownego złożenia oferty cenowej na Zadanie nr 1.

8.5.

9. **Istotne warunki zamówienia:**

9.1. Z uwagi na fakt, iż projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego na wykonawcę nałożone zostaną poniższe obowiązki:

9.1.1. obowiązek udostępnienia na każde żądanie dokumentacji, w tym dokumentacji finansowej, związanej z realizacją zamówienia;

9.1.2. obowiązek stosowania dokumentacji wskazanej przez zamawiającego;

9.1.3. obowiązek przyjęcia ewentualnych zmian szczegółowego zakresu zamówienia w wyniku zmiany wymogów formalnych związanych z realizacją Projektu.

9.2. Odbiór końcowy nastąpi po zakończeniu wszystkich niezbędnych prac na Infrastrukturze uzgodnionej z Zamawiającym.

9.3. Odbiór końcowy przedmiotu zamówienia dla Zadania nr 1 nastąpi nie później niż 14.08.2023 r.

10. **Pozostałe postanowienia:**
    10.1. zamawiający nie dopuszcza składanie ofert częściowych;
    10.2. zamawiający nie dopuszcza składania ofert wariantowych;
    10.3. dowodem prawidłowej realizacji zamówienia będzie podpisany bez uwag przez osobę odbierającą przedmiot zamówienia protokół odbioru;
    10.4. zamawiający zastrzega sobie prawo podjęcia negocjacji oferowanych warunków z wykonawcą, którego oferta uznana została za najkorzystniejszą w celu uzyskania warunków korzystniejszych dla zamawiającego;
    10.5. zamawiający zastrzega sobie prawo do unieważnienia postępowania w następujących przypadkach
        1) nie złożono żadnej oferty niepodlegającej odrzuceniu;
        2) cena najkorzystniejszej oferty lub cena oferty z najniższą ceną przewyższa kwotę, którą zamawiający zgodnie z budżetem Projektu może przeznaczyć na sfinansowanie zamówienia, chyba że zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty;
        3) wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć;
        4) postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie niepodlegającej unieważnieniu umowy w sprawie zamówienia publicznego;
    10.6. w przypadku uznania oferty za najkorzystniejszą, wykonawca zobowiązuje się do zawarcia umowy na zadanie nr 1 w miejscu i terminie wskazanym przez zamawiającego;
    10.7. zamawiający zastrzega sobie prawo do wydłużenia terminu realizacji zamówienia w przypadku wydłużenia terminu realizacji projektu, na rzecz którego świadczone będą usługi.
    10.8. Zamawiający zastrzega sobie prawo do wycofania zapytania ofertowego bez podania przyczyny.

11. **Tryb udzielania wyjaśnień:**
    11.1. wykonawca może zwrócić się do zamawiającego o wyjaśnienia dotyczące niniejszego zapytania, a zamawiający udzieli ich bez zbędnej zwłoki.
    11.2. Zamawiający dopuszcza następujące formy zapytań i udzielania wyjaśnień:
        11.2.1. pisemna, na adres: SAMODZIELNA PUBLICZNA PRZYCHODNIA WIEJSKA GMINY CHOJNICE , 89-600 Chojnice, ul. Kościerska 9
        11.2.2. za pośrednictwem poczty elektronicznej, na adres: informatyk1@przychodniawiejska.pl

12. **Załączniki:**
    12.1. Załącznik nr 1 zawierający formularz oferty, oświadczenie wykonawcy o spełnianiu warunków udziału w postępowaniu, oświadczenie wykonawcy o braku powiązań kapitałowych lub osobowych oraz oświadczenie o wykluczeniu;
    12.2. Załącznik nr 2 klauzula informacyjna dotycząca przetwarzania danych osobowych.