Poznań, 21 grudnia 2018 r.

ZAPYTANIE OFERTOWE

na obsługę informatyczną Wielkopolskiego Funduszu Rozwoju sp. z o.o. z siedzibą w Poznaniu

1. INFORMACJE O ZAMAWIAJĄCYM:

Wielkopolski Fundusz Rozwoju sp. z o.o.
ul. Szyperska 14, 61-754 Poznań
tel. +48 61 671 71 71
e-mail: wfr@wfr.org.pl
NIP: 783-17-49-000, REGON: 365658047

2. PRZEDMIOT ZAMÓWIENIA:

Przedmiotem zamówienia jest świadczenie usług z zakresu obsługi informatycznej w siedzibie Zamawiającego.

Podstawowe informacje:

- podpisanie umowy w terminie 3 dni roboczych od chwili wyboru oferty,
- przewidywany termin realizacji zamówienia - od 1 stycznia 2019 roku do 31 grudnia 2019 roku,
- realizacja zamówienia w siedzibie Zamawiającego w dni robocze w godzinach od 7:30 do 15:30,
- liczba stanowisk komputerowych – 47 stanowisk komputerowych na początku 2019 roku, w okresie późniejszym sukcesywny wzrost do planowanych 52 stanowisk komputerowych do końca grudnia 2019 roku.

3. OPIS PRZEDMIOTU ZAMÓWIENIA:

Wielkopolski Fundusz Rozwoju sp. z o.o. zwraca się z prośbą o przesłanie oferty cenowej na obsługę informatyczną Spółki.

Kompleksowa obsługa informatyczna w zakresie obecnej i docelowej infrastruktury informatycznej Zamawiającego powinna spełniać następujące wymagania:

A. Zakres wykonywanych prac

1) nadzór nad działaniem sieci komputerowej;
2) administracja stacjami roboczymi (zarządzanie użytkownikami, usuwanie błędów programowych w systemach operacyjnych jak i aplikacjach użytkowych, stosowanie polityki bezpieczeństwa tzn. cotygodniowa archiwizacja danych, kontrola logów, sukcesywne wgrywanie poprawek systemowych;

3) administracja serwerem Windows 2016 (Kontroler domeny, Serwer plików, Serwer drukarek, Serwer DHCP, Serwer DNS, Serwer oprogramowania finansowo-księgowego) oraz stosowanie polityki bezpieczeństwa tzn. codzienna archiwizacja danych, kontrola logów oraz innych komunikatów serwerów na temat ich pracy, sukcesywne wgrywanie poprawek systemowych);
4) administracja i zarządzanie ochroną antywirusową firmy ESET NOD32 Antivirus Business Edition:
   a) zarządzanie licencjami oraz informacje o wygasających lub nie wykorzystanych licencjach,
   b) skanowanie dysków stacji roboczych i serwerów w poszukiwaniu zagrożeń,
   c) dostosowanie konfiguracji klienta oprogramowania antywirusowego, antyspyware firmy ESET,
   d) instalacja aktualizacji lub nowego oprogramowania zabezpieczającego do dowolnego komputera i serwera w sieci w celu zapewnienia pełnej ochrony,
   e) cotygodniowa aktualizacja bazy danych programów antywirusowych NOD 32 wersja serwerowa 50 licencji;
5) administracja siecią komputerową:
   a) ul. Szyperska 14, 6 piętro, router Drytek , UTM STORMSHIELD SN310, switche TP –Link 3 warstwy PoE 4 szt.,
   b) ul. Szyperska14, 5 piętro, switche TP –Link 3 warstwy PoE 2 szt.;
6) sprawdzanie poprawności wysyłanych i odbieranych pakietów, konfiguracja nowych połączeń LAN, WAN;
7) rozbudowa sieci, zmiany stacji roboczych i wprowadzanie zmian w oprogramowaniu systemowym;
8) usuwanie błędów programowych na stacjach roboczych;
9) usuwanie błędów programowych i sprzętowych w sieci;
10) porady i szkolenia z zakresu obsługi stacji roboczych, systemu operacyjnego, poczty elektronicznej, programów biurowych na stanowiskach roboczych WFR;
11) bieżąca kontrola konfiguracji komputerów oraz legalności oprogramowania i usuwanie wszelkich nieprawidłowości w tym zakresie;
12) instalacja i konfiguracja oprogramowania systemowego i biurowego;
13) rekonfiguracja systemów operacyjnych i oprogramowania biurowego (sukcesywne wgrywanie poprawek systemowych);
14) usuwanie błędów systemowych na stacjach roboczych na bieżąco;
15) telefoniczna pomoc techniczna;
16) ewidencja sprzętu komputerowego i oprogramowania;
17) zapewnianie ciągłości działania systemów informatycznych;
18) zarządzanie serwisem Internetowym;
19) praca koncepcyjna nad rozwojem i rozbudową systemów komputerowych w WFR Poznań.

B. Obsługa i utrzymanie strony internetowej oraz kont pocztowych

Serwis strony WWW:

1) usługi główne**:**
   a) nieograniczona ilość domen z przekierowaniem na podkatalogi,
   b) nieograniczona ilość subdomen z przekierowaniem na podkatalogi,
   c) utrzymanie serwerów DNS,
   d) baza danych (MySQL lub PostgreSQL),
   e) nieograniczony transfer miesięcznie,
   f) nieograniczona powierzchnia dysku,
   g) łącze min. 500 Mb/s;
2) usługi pocztowe:
   a) nieograniczona ilość kont pocztowych,
   b) serwery poczty we własnej domenie (POP3, SMTP, IMAP),
   c) system antywirusowy,
   d) inteligentny system antyspamowy (+ whitelista i blacklista osobno dla każdego konta pocztowego),
   e) autoryzacja SMTP - antyoszust,
   f) nieograniczona ilość aliasów pocztowych,
   g) nieograniczona ilość autoresponderów,
   h) nieograniczona ilość kont z opcją Forward - przekazywanie poczty na inne konta,
   i) nieograniczona ilość list pocztowych;
3) usługi FTP - własne konto FTP;
4) dostęp do:
   a) CGI,
   b) PHP,
   c) Perl,
   d) Python,
   e) WAP,
   f) SSI;
5) narzędzia:
   a) administracja wszystkimi usługami pocztowymi w domenie,
   b) administracja pojedynczym kontem pocztowym,

c) graficzne statystyki oglądalności stron,

d) domyślnie instalowane skrypty CGI (formularz, licznik, guest book, chatroom, mini wyszukiwarka zawartości stron),

e) CRM Kreator stron WWW;

6) bezpieczeństwo:

a) codzienna kopia bezpieczeństwa,

b) pełne logi serwera,

c) katalogi na hasło,

d) system firewall,

e) pomoc i nadzór administratora 24h/dobę.

C. Tworzenie backupu oraz zarządzanie plikami i zadaniami backupu i ich monitoring poprzez oprogramowanie ShadowProtect

1) tworzenia polityk backupu dla różnych grup urządzeń;

2) okresowa weryfikacja obrazów backupu;

3) ustalania specyficznych reguł powiadomień dotyczących środowiska backupowego;

4) raportowanie o stanie systemie i backupu na wszystkich urządzeniach Zamawiającego;

5) wdrażanie polityki konsolidacji obrazu backupu

6) zarządzenie replikacją backupu przez LAN i WAN.

D. Szyfrowanie danych w oparciu o ustalone polityki

1) tworzenie polityki szyfrowania w konsoli centralnego zarządzania,

2) zarządzanie zaszyfrowanymi stacjami, użytkownikami oraz kluczami szyfrującymi,

3) zarządzanie kluczami szyfrującymi polegającym na bezpiecznym dodawaniu lub usuwaniu kluczy szyfrujących, a także zmianę polityki bezpieczeństwa.

E. Zarządzanie urządzeniem klasy UTM STORMSHIELD SN310

F. Pełnienie obowiązków Administratora Systemów Informatycznych – ASI:

1) wspomaganie Inspektora Ochrony Danych w opracowaniu i aktualizacji polityki bezpieczeństwa w zakresie zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych, a także wszelkiej dokumentacji dotyczącej ochrony danych osobowych;

2) systematyczne kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;

3) dostosowywanie systemów informatycznych służących przetwarzaniu danych osobowych do wymogów rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO);

4) zarządzanie funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych;

5) zarządzanie hasłami użytkowników i nadzorze nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi zawartymi w instrukcji zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji;

6) sprawdzanie systemu pod kątem obecności wirusów komputerowych oraz sprawdzanie częstości i poprawności wykonywania procedur uaktualniania systemów antywirusowych;

7) wykonanie kopii awaryjnych, ich przechowywanie i okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu;

8) zapewnienie, aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby komputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych;

9) dokonywanie analizy zagrożeń dla bezpieczeństwa danych osobowych oraz wdrażaniu zmian w Polityce Bezpieczeństwa w celu zapewnienia właściwego poziomu ochrony przetwarzanych danych osobowych;

10) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych;

11) nadzorowanie przeglądów, konserwacji oraz uaktualnianie systemów służących do przetwarzania oraz wszystkimi innymi czynnościami wykonywanymi na zbiorach danych osobowych;

12) sporządzanie raportu naruszenia bezpieczeństwa systemu informatycznego;

13) informowanie Zamawiającego - Administratora Danych Osobowych o awariach uniemożliwiających normalne funkcjonowanie systemu informatycznego, dostrzeżonych przypadkach naruszenia instrukcji przez użytkowników, a w szczególności o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych;

14) na żądanie Zamawiającego - Administratora Danych Osobowych, przekładaniu przygotowanej wspólnie z Inspektorem Ochrony Danych kompleksowej analizy zarządzania systemem informatycznym;

15) bieżące informowanie na piśmie Zamawiającego - Administratora Danych Osobowych o wszelkich stwierdzonych nieprawidłowościach w zakresie zgodności przetwarzania danych osobowych z przepisami prawa;

16) po otrzymaniu informacji o podejrzeniu naruszenia zasad ochrony danych osobowych, w porozumieniu z Inspektorem Ochrony Danych: weryfikowaniu metody pracy osób upoważnionych do przetwarzania danych, weryfikowaniu stan urządzeń wykorzystywanych do przetwarzania danych, weryfikowaniu sposób działania systemu operacyjnego, weryfikowaniu jakości połączeń

w sieci lokalnej Spółki i jakości połączenia z siecią Internet, weryfikowaniu zawartość zbioru danych i podejmowaniu odpowiednich środków w celu przywrócenia stanu zgodnego z prawem.

Pozostałe obowiązki Wykonawcy zostały określone we Wzorze Umowy, stanowiącym nr 1 do Zapytania ofertowego.

4. WYMAGANIA DOTYCZĄCE WYKONAWCY:

1) oferty mogą składać Wykonawcy, którzy w okresie ostatnich trzech lat przed upływem terminu składania ofert, wykonali lub wykonują co najmniej dwie usługi polegające na kompleksowej obsłudze informatycznej na rzecz podmiotów, dysponujących co najmniej 30 stanowiskami komputerowymi oraz co najmniej jedną usługę polegającą na pełnieniu funkcji administratora systemów informatycznych, przez okres co najmniej jednego roku w odniesieniu do każdej usługi;
2) w celu wykazania spełniania przez Wykonawcę warunku, o którym mowa w pkt 1, Zamawiający wymaga przedstawienia aktualnego na dzień składania ofert Oświadczenia Wykonawcy o spełnianiu powyższego warunku. Wzór przedmiotowego Oświadczenia Wykonawcy stanowi załącznik nr 2 do Zapytania ofertowego.

5. OPIS SPOSOBU PRZYGOTOWANIA OFERTY:

1) oferta powinna zostać sporządzona według wzoru formularza ofertowego, stanowiącego załącznik nr 3 do Zapytania ofertowego;
2) na sporządzonej ofercie powinien znajdować się podpis osoby upoważnionej do reprezentowania Wykonawcy;
3) Wykonawca wskazuje w ofercie cenę brutto, cenę netto oraz podatek VAT;
4) cena oferty winna zawierać ostateczną kwotę, która uwzględniać powinna wszelkie koszty bezpośrednie i pośrednie związane z wykonaniem przedmiotu zamówienia, w tym m.in. koszty wykonania i dostarczenia przedmiotu zamówienia, zysk Wykonawcy oraz wszystkie wymagane przepisami podatki oraz opłaty;
5) rozliczenie transakcji następować będzie przelewem na konto wskazane na fakturze w ciągu 14 dni od daty otrzymania prawidłowo wystawionej faktury przez Wykonawcę.

6. MIEJSCE I TERMIN SKŁADANIA OFERT:

Oferta powinna zostać sporządzona według wzoru Formularza ofertowego, stanowiącego Załącznik nr 3 do Zapytania ofertowego.

Ofertę należy przesłać w wersji elektronicznej (skan formularza ofertowego, ewentualnie skan pełnomocnictwa w przypadku gdy ofertę składa osoba upoważniona do dokonywania czynności w imieniu Wykonawcy, skan oświadczenia Wykonawcy) na adres: wfr@wfr.org.pl lub

dostarczyć w wersji papierowej do siedziby Zamawiającego: ul. Szyperska 14, 61-754 Poznań z dopiskiem „Zapytanie ofertowe na obsługę informatyczną Wielkopolskiego Funduszu Rozwoju sp. z o.o. z siedzibą w Poznaniu w roku 2019”.

w terminie do **dnia 28 grudnia 2018 r. do godz. 12.00.**

Wymagany termin związania ofertą: 30 dni.

7. ROZSTRZYGNIĘCIE POSTĘPOWANIA:

1) oferty, które wpłyną po wyznaczonym terminie złożenia, nie będą brane pod uwagę przy ocenie ofert;
2) Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyny;
3) Zamawiający zastrzega sobie możliwość odrzucenia oferty, która nie spełnia wymagań określonych w Zapytaniu ofertowym;
4) Zamawiający zastrzega sobie możliwość poprawiania oczywistych omyłek pisarskich i rachunkowych;
5) w przypadku zaistnienia szczególnych okoliczności Zamawiający dopuszcza możliwość przedłużenia terminu realizacji zamówienia, jednakże ocena, czy zachodzą szczególne okoliczności, zależy wyłącznie od decyzji Zamawiającego.

8. KRYTERIUM OCENY OFERT:

Wybór najkorzystniejszej oferty spośród ofert niepodlegających odrzuceniu zostanie przeprowadzony w oparciu o następujące kryteria:

Nr	Nazwa kryterium	Waga
1.	Łączna cena za wykonanie przedmiotu zamówienia w okresie od 1 stycznia 2019 roku do 31 grudnia 2019 roku	70%
2.	Czas reakcji na zgłoszenie serwisowe Zamawiającego	15%
3.	Certyfikaty potwierdzające wiedzę Wykonawcy w zakresie administrowania systemami informatycznymi	15%

1) Cena (C) – 70%, maksymalna liczba punktów: 70

Liczba punktów w tym kryterium zostanie obliczona wg następującego wzoru:

$$C = \frac{C_n}{C_{bo}} \times 70$$

gdzie:

C – liczba punktów w kryterium „Cena”

C_n – najniższa cena ofertowa brutto spośród badanych ofert,

C_{bo} – cena brutto badanej oferty.

2) Czas reakcji na zgłoszenie serwisowe Zamawiającego (CzR) w przypadku wystąpienia awarii krytycznej – 15%, maksymalna liczba punktów: 15

Czas reakcji na zgłoszenie serwisowe Zamawiającego w przypadku wystąpienia awarii krytycznej to czas, w którym Wykonawca zobowiązany jest podjąć czynności mające na celu jej usunięcia.

Przez awarię krytyczną należy rozumieć awarię uniemożliwiającą normalne funkcjonowanie infrastruktury informatycznej Zamawiającego.

Zamawiający wymaga, aby czas reakcji na zgłoszenie serwisowe Zamawiającego nie był dłuższy niż 4 godziny (pod rygorem odrzucenia oferty), licząc od momentu przekazania przez Zamawiającego takiego zgłoszenia.

W ramach tego kryterium (CzR), oferty będą ocenione w taki sposób, że Zamawiający przyzna następującą ilość punktów:

a) za zaoferowany czas reakcji do dwóch godzin od przekazania zgłoszenia Zamawiającego: 15 pkt,

b) za zaoferowany czas reakcji do trzech godzin od przekazania zgłoszenia Zamawiającego: 10 pkt,

c) za zaoferowany czas reakcji do czterech godzin od przekazania zgłoszenia Zamawiającego: 0 pkt.

3) Certyfikaty potwierdzające wiedzę z zakresu administrowania systemami informatycznymi (CW) – 15%, maksymalna liczba punktów – 15

W ramach rzeczonego kryterium ocenie podlega posiadanie przez Wykonawcę certyfikatów potwierdzających wiedzę z zakresu administrowania (certyfikat powinien być wystawiony przez podmiot niezależny) - Windows Serwer, UTM STORMSHIELD SN310 oraz oprogramowaniem do backapu ShadowProtect.

Oferty będą oceniane w następujący sposób:

a) posiadanie certyfikatu potwierdzającego wiedzę z zakresu administrowania Windows Serwer – 5 pkt,
b) posiadanie certyfikatu potwierdzającego wiedzę z zakresu administrowania UTM STORMSHIELD SN310 – 5 pkt,
c) posiadanie certyfikatu potwierdzającego wiedzę z zakresu administrowania oprogramowaniem do backapu ShadowProtect – 5 pkt.

Oceny punktowe uzyskane w wyżej wymienionych kryteriach sumuje się, a uzyskana łączna liczba punktów stanowić będzie całkowitą oceną punktową oferty (L).

Łączna ocena punktowa liczona będzie z dokładnością do dwóch miejsc po przecinku. Liczba punktów zostanie obliczona według następującego wzoru:

L = C + CzR + CW

Wybrana zostanie oferta, która uzyska największą (łączną we wszystkich kryteriach) liczbę punktów (L).

Jeżeli nie można wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z niższą ceną,

a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

9. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

W związku z składanymi ofertami informujemy, że:

1) administratorem danych osobowych jest Wielkopolski Fundusz Rozwoju sp. z o.o. z siedzibą w Poznaniu ul. Szyperska 14, 61-754 Poznań;
2) w sprawach związanych z przetwarzaniem danych osobowych można kontaktować się z inspektorem ochrony danych osobowych, ul. Szyperska 14, 61-754 Poznań, adres email iod@wfr.org.pl;
3) dane osobowe oferentów są przetwarzane w celach wyboru najkorzystniejszej oferty, zawarcia i rozliczenia umowy oraz archiwizacji dokumentów;
4) podstawa prawna przetwarzania danych osobowych oferentów:
   a) na podstawie art. 6 ust. 1 lit. b RODO w związku z zawarciem oraz wykonaniem umowy, której oferent jest stroną;
   b) na podstawie art. 6 ust. 1 lit. c RODO w związku z wypełnieniem obowiązku prawnego ciążącym na administratorze, w tym rozliczenia finansowo podatkowego zawieranej umowy oraz obowiązków wynikających z ustawy o finansach publicznych;
5) dane osobowe oferentów będą przetwarzane przez okres 10 lat;
6) podanie danych osobowych jest warunkiem zawarcia umowy lub podjęcia działań niezbędnych przed jej zawarciem;
7) oferentom przysługuje:
   a) prawo do przenoszenia danych, w przypadku gdy dane są przetwarzane w związku wykonaniem umowy i gdy dane te są przetwarzane w sposób zautomatyzowany,
   b) prawo do dostępu do danych osobowych, ich sprostowania lub ograniczenia przetwarzania,
   c) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8) dane osobowe oferentów nie będą ujawniane podmiotom innym niż upoważnione na podstawie przepisów prawa;
9) dane osobowe nie będą przetwarzane w sposób zautomatyzowany w celu podjęcia jakiejkolwiek decyzji, w tym profilowaniu.

10. OSOBY UPOWAŻNIONE DO KONTAKTU:

Piotr Łykowski

piotr.lykowski@wfr.org.pl

PREZES ZARZĄDU

/-/ Hubert Zobel

WICEPREZES ZARZĄDU

/-/ Jarosław Sierszchulski

Załączniki:

1) Wzór Umowy.
2) Oświadczenie Wykonawcy o spełnianiu warunku udziału w postępowaniu;
3) Formularz ofertowy.