SAMORZĄD WOJEWÓDZTWA WIELKOPOLSKIEGO

Wielkopolski Fundusz Rozwoju
Spółka Samorządu Województwa Wielkopolskiego

Poznań, 21 grudnia 2017 r.

ZAPYTANIE OFERTOWE

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

w roku 2018

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:

- zawarcie umowy w terminie 3 dni roboczych od chwili wyboru oferty,
- przewidywany termin realizacji zamówienia - od 1 stycznia 2018 roku do 31 grudnia 2018 roku,
- realizacja zamówienia w siedzibie Zamawiającego w dni robocze w godzinach od 7:30 do 15:30,
- liczba stanowisk komputerowych – 35 stanowisk komputerowych na początku 2018 roku, w okresie późniejszym, sukcesywny wzrost do planowanych 40 stanowisk komputerowych do końca grudnia 2018 roku.

3. OPIS PRZEDMIOTU ZAMÓWIENIA

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 2012 (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 niewykorzystanych 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 - 35 licencji;
5) administracja siecią komputerową:
   a) ul. Szyperska 14, 6 piętro, router Drytek , switche TP –Link 3 warstwy PoE 4 szt.,
   b) ul. Szyperska 14, parter, router Drytek, switche TP –Link 3 warstwy PoE 1 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 Zamawiającego.

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, miniwyszukiwarka 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:

1) tworzenie polityk backupu dla różnych grup urządzeń;
2) okresowa weryfikacja obrazów backupu;
3) ustalania specyficznych reguł powiadomień dotyczących środowiska backupowego;
4) raportowanie o stanie systemu 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, polegające na bezpiecznym dodawaniu lub usuwaniu kluczy szyfrujących, a także zmianę polityki bezpieczeństwa.

E. Zarządzanie urządzeniem klasy UTM.

F. Pełnienie obowiązków Administratora Systemów Informatycznych – ASI:

1) wspomaganie Administratora Bezpieczeństwa Informacji w opracowaniu i aktualizacji Instrukcji Zarządzania Systemem Informatycznym, służącym 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) dostosowanie wszystkich systemów informatycznych, służących przetwarzaniu danych osobowych do wymogów rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100., poz. 1024) oraz dostosowanie wszystkich systemów informatycznych, służących przetwarzaniu danych osobowych do wymogów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE z 2016 r., seria L, Nr 119, poz. 1);

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

5) zarządzanie hasłami użytkowników i nadzór 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 wdrażanie zmian w Polityce Bezpieczeństwa Zamawiającego, 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 wszystkich innych czynności wykonywanych na zbiorach danych osobowych;

12) sporządzanie raportu naruszenia bezpieczeństwa systemu informatycznego;

13) informowanie 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 Administratora Danych Osobowych, przekładanie przygotowanej wspólnie z Administratorem Bezpieczeństwa Informacji kompleksowej analizy zarządzania systemem informatycznym;

15) bieżące informowanie na piśmie 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 Administratorem Bezpieczeństwa Informacji, weryfikowanie metody pracy osób upoważnionych do przetwarzania danych, weryfikowanie stanu urządzeń wykorzystywanych do przetwarzania danych, weryfikowanie sposobu działania systemu operacyjnego, weryfikowanie jakości połączeń w sieci lokalnej Zamawiającego i jakości połączenia z siecią Internet, weryfikowanie zawartości zbioru danych i podejmowanie odpowiednich środków w celu przywrócenia stanu zgodnego z prawem.

4. WYMAGANIA DOTYCZĄCE WYKONAWCY:

1) oferty mogą składać Wykonawcy, którzy w okresie ostatnich trzech lat przed upływem terminu składania ofert, należycie wykonali lub wykonują co najmniej jedną usługę polegającą na kompleksowej obsłudze informatycznej podmiotu, dysponującego co najmniej 20 stanowiskami komputerowymi, przez okres co najmniej jednego roku;
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 niniejszego Zapytania ofertowego.

5. MIEJSCE I TERMIN SKŁADANIA OFERT:

Oferta powinna zostać sporządzona według wzoru Formularza ofertowego, stanowiącego Załącznik nr 1 do niniejszego Zapytania ofertowego.

Ofertę wraz z Oświadczeniem Wykonawcy o spełnianiu warunku udziału w postępowaniu wraz z pełnomocnictwem, uprawniającym do złożenia oświadczenia woli (jeżeli takie zostało udzielone) należy przesłać w wersji elektronicznej (skan **Formularza ofertowego**, skan **Oświadczenia Wykonawcy,** skan **pełnomocnictwa**) na adres:

wfr@wfr.org.pl w terminie do dnia 28 grudnia 2017 r. do godz. 13:00.

Wymagany termin związania ofertą: 21 dni.

6. ROZSTRZYGNIĘCIE POSTĘPOWANIA:

1) oferty, które wpłyną po wyznaczonym terminie złożenia nie będą brane pod uwagę przy ocenie ofert;
2) Zamawiający zastrzega sobie prawo odstąpienia od realizacji zamówienia;
3) Zamawiający zastrzega sobie możliwość odrzucenia oferty, która nie spełnia wymagań Zamawiającego;
4) w przypadku zaistnienia szczególnych okoliczności, Zamawiający dopuszcza możliwość przedłużenia terminu realizacji zamówienia, jednakże ocena, czy zachodzą szczególne okoliczności należy wyłącznie od decyzji Zamawiającego.

7. 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 2018 roku do 31 grudnia 2018 roku	80%
2.	Czas reakcji na zgłoszenie Zamawiającego w przypadku wystąpienia awarii krytycznej	20%

1) **Cena (C) – 80%, maksymalna liczba punktów: 80**

Liczba punktów w tym kryterium zostanie obliczona wg następującego wzoru:

$$C = \frac{C_n}{C_{bo}} \times 80$$

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 Zamawiającego (CzR) w przypadku wystąpienia awarii krytycznej – 20%, maksymalna liczba punktów: 20**

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

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

Zamawiający wymaga, aby czas reakcji na zgłoszenie 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: 20 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.

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

Wybrana zostanie oferta, która uzyska największą (łącznie 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.

8. OSOBY UPOWAŻNIONE DO KONTAKTU:

Piotr Łykowski

piotr.lykowski@wfr.org.pl

WICEPREZES ZARZĄDU

Jarosław Sierszchulski

Załączniki:

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