Zapytanie ofertowe

Postępowanie prowadzone w oparciu o art. 4 pkt. 8 ustawy z dnia 29 stycznia 2004 r.
Prawo zamówień publicznych
/tj. Dz. U. z 2013 r. poz. 907 ze zm./

I. Zamawiający: **Powiatowy Urząd Pracy w Wołowie**

Adres do korespondencji: Plac Piastowski 2, 56-100 Wołów

tel. 0-71 389 10 92, faks 0-71 389 26 55

Zaprasza do złożenia ofert cenowych na:
Audyt i modyfikacja systemu zarządzania bezpieczeństwem informacji

II. Opis przedmiotu zamówienia

1. Wykonanie audytu obowiązującego w Powiatowym Urzędzie Pracy systemu zarządzania bezpieczeństwem informacji.

a) Weryfikacja zgodności z obowiązującymi aktami prawnymi, a w szczególności z:

- Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2015 r. poz. 2135, z późniejszymi zmianami),

- Ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005r. (Dz. U. 2005 nr 64, poz. 565 z późniejszymi zmianami)

- Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiada urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,

- Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 r. (Dz.U. 2016 poz. 113),

b) Weryfikacja zgodności z obowiązującą normą:

- PN-ISO/IEC 27001 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania”

c) Utworzenie raportu zawierającego niezgodności oraz zalecenia do wdrożenia.

2. Wykonanie testów penetracyjnych wewnętrznych i zewnętrznych. Opracowanie raportu zawierającego wykryte zagrożenia oraz zalecenia do zastosowania przy konfiguracji urządzeń sieciowych. Weryfikacja i analiza:

- bezpieczeństwa dostępu do wewnętrznej infrastruktury sieciowej IT.

- odporności infrastruktury IT na bezautoryzacyjne rozpoznanie jego składowych, w tym weryfikacja podatności serwisów DNS.

- systemów oraz protokołów zarządzania i monitorowania infrastruktury IT.

- ochrony przed oprogramowaniem szkodliwym poprzez próby propagacji testowego oprogramowania szkodliwego. (z wewnątrz infrastruktury IT).

- poufności i integralności przetwarzania danych w systemach bazodanowych, w szczególności

danych osobowych.

- identyfikacji oraz autentykacji stosowanych w mechanizmach autoryzacji dostępu do zasobów IT.
- podatności systemów i sieci na ataki takie jak sniffing, spoofing, man-in-the-middle.
- otwartości portów, podatności związanych z autoryzacją dostępu zdalnego do zasobów IT i ocena związanych z tym ryzyk.
- bezautoryzacyjnego dostępu do informacji o rodzaju i wersji wykorzystywanego oprogramowania systemowego i usługowego.
- podatności hostów na ataki w warstwie systemowej (przy wykorzystaniu exploitów).
- podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych.
- poufności przesyłu danych przetwarzanych na udostępnionych zasobach plikowych.
- bezautoryzacyjnej dostępności do danych o czasie pracy, krytycznych systemów.
- obecności domyślnych kont użytkowników oraz haseł.
- poufności przesyłania danych do wydruku
- podatności systemu sieci wewnętrznej na zakłócenie/zablokowanie dostępności do usług i określenie zasięgu oraz zlokalizowanie fizycznego źródła ataku.
- poufności i czasu podtrzymania danych autoryzacyjnych aplikacji www.

3. Wykonanie aktualizacji istniejącego systemu zarządzania bezpieczeństwem informacji ze szczególnym uwzględnieniem zaleceń określonych w punktach 1c i 2.

W opracowaniu mają być wzięte pod uwagę następujące zagadnienia:

- Wymagania w zakresie zabezpieczeń teleinformatycznych
- Zasady bezpiecznego przetwarzania informacji przez pracowników Zamawiającego
- Stosowanie zasady czystego biura i czystego ekranu
- Zabezpieczenie stacji roboczych
- Zasady klasyfikacji informacji i postępowania z informacjami klasyfikowanymi
- Zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień
- Zasady zarządzania dostępem do usług informatycznych, w tym usług sieciowych
- Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami
- Zasady publikacji informacji
- Zasady wymiany danych z podmiotami zewnętrznymi
- Zasady wewnętrznej wymiany danych
- Zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach

4. Wdrożenie konfiguracji switchy, routerów, serwerów i innych urządzeń podłączonych do sieci komputerowej PUP ograniczających zagrożenia wykryte w punkcie 2.

5. Przeprowadzenie szkolenia dla pracowników i stażystów obejmującego zmodyfikowaną dokumentacje dotyczącą zarządzania bezpieczeństwem informacji.

- Omówienie podstawowych zasad bezpieczeństwa informacji i wypełniania procedur bezpieczeństwa informacji
- Zagrożenia związane z przetwarzaniem informacji
- Odpowiedzialność za naruszenie zasad bezpieczeństwa informacji;
- Zasady zgłaszania i procedury reagowania na incydenty.

Wykonawca przekaże Zamawiającemu materiały szkoleniowe i prezentacje z przeprowadzonych szkoleń.

6. Wykonanie inwentaryzacji posiadanych oraz użytkowanych licencji. Utworzenie raportu zawierających braki w licencjach wraz z zalecanymi działaniami naprawczymi.

III. Wymagania dodatkowe

1. Wykonawca związany jest ofertą 14 dni.

2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

3. **Wymagany termin realizacji zamówienia: 30 dni od podpisania umowy, nie później niż do 10.12.2016 r.**

IV. Dokumenty, jakie Wykonawca powinien załączyć do oferty:

1. Zamawiający wymaga, aby każda oferta zawierała minimum następujące dokumenty:

1) wypełniony i podpisany przez Wykonawcę formularz cenowo-ofertowy – wg. załączonego wzoru formularza ofertowego,

2) Aktualny odpis z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt.2 ustawy, wystawiony nie wcześniej niż **6 miesięcy** przed upływem terminu składania ofert **(załącznik Wykonawcy);**

3) Referencje potwierdzające prawidłowe wykonanie audytów w ciągu ostatnich 3 lat

4) Potwierdzenie posiadania, co najmniej jednego z poniższych certyfikatów:

a) Audytor Wiodący ISO 27001:2013 akredytowany przez IRCA

b) Certified Information Systems Security Professional (CISSP) lub certyfikat ukończenia akredytowanego szkolenia CISSP przez ISC2

c) NSE4

d) PRINCE 2

e) Administrator bezpieczeństwa informacji

V. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów.

1. Wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy mogą przekazywać pisemnie, za pomocą faksu lub drogą elektroniczną.

2. Osoby po stronie Zamawiającego uprawnione do porozumiewania się z Wykonawcami

a) Osobą uprawnioną do kontaktowania się z Wykonawcami i udzielania wyjaśnień dotyczących postępowania w jest Pan Cezary Rytwiński e-mail: cezary.rytwinski@pupwolow.pl

b) Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie istotnych warunków udzielenia zamówienia w godzinach pracy urzędu tj.: 7:45-15:45.

VII. Miejsce składania ofert

Ofertę cenową należy:

- złożyć w siedzibie Zamawiającego w zamkniętej kopercie z dopiskiem „Modernizacja sieci komputerowej Powiatowego Urzędu Pracy w Wołowie" NIE OTWIERAĆ PRZED 4.11.2016 r.

- przesłać drogą elektroniczną adres e-mail cezary.rytwinski@pupwolow.pl

w terminie do dnia 4.11.2016 , godz 12:00

VIII. Opis sposobu obliczania ceny

1. Na załączonym formularzu cenowo-ofertowym, należy przedstawić cenę ofertową brutto za wykonanie / udzielenie przedmiotu zamówienia.
2. Wartość cenową należy podać w złotych polskich cyfrą – z dokładnością do dwóch miejsc po przecinku oraz słownie.
3. Cena powinna zawierać wszelkie koszty związane z wykonaniem przedmiotu zamówienia.
4. Wszelkie rozliczenia pomiędzy Zamawiającym a Wykonawcą odbywać się będą w złotych polskich.

VIII. Informacje o formalnościach

1. Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający zawiadomi wszystkich Wykonawców, którzy ubiegali się o udzielenie zamówienia o wyniku postępowania.
2. Zamawiający zawrze umowę z wybranym Wykonawcą po przekazaniu zawiadomienia o wyborze Wykonawcy, ale nie później niż w terminie związania ofertą.
3. Jeżeli Wykonawca, którego oferta została wybrana uchyli się od zawarcia umowy, Zamawiający wybierze kolejną ofertę najkorzystniejszą spośród złożonych ofert, bez przeprowadzania ich ponownej oceny.
4. Do prowadzonego postępowania nie przysługują Wykonawcom środki ochrony prawnej określone w przepisach Ustawy Prawo zamówień publicznych tj. odwołanie, skarga.
5. Niniejsze postępowania prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach organizacyjnych Zamawiającego. Nie mają w tym przypadku zastosowania przepisy Ustawy Prawo zamówień publicznych.
6. **Zamawiający zastrzega sobie prawo odrzucenia oferty, bez wezwania do uzupełnienia, w przypadku nie dostarczenia kompletu wymaganych dokumentów.**

Załączniki:

1. Formularz ofertowo-cenowy

ZATWIERDZIŁ:

…..……..

(podpis i pieczęć
osoby zatwierdzającej postępowanie)