Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Mława dnia 27.09.2022 r.

Znak sprawy: WI.271.49.2022

Zapytanie ofertowe

na przeprowadzenie ***„Przeprowadzenie szkolenia dla pracowników urzędu Miasta Mława (stacjonarne) w zakresie obsługi zakupionego sprzętu i oprogramowania w ramach umowy o powierzenie grantu o numerze 4639/3/2022" w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.***

Rozdział I. ZAMAWIAJĄCY
Miasto Mława
ul. Stary Rynek 19
06-500 Mława
tel. (23) 654 32 51 wew. 100
e-mail: info@mlawa.pl

Rozdział II. TRYB ZAMÓWIENIA, PODSTAWA PRAWNA

1. Tryb zamówienia
Do niniejszego postępowania nie ma zastosowania ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm.) – wyłączenie stosowania ustawy zgodnie z brzmieniem art. 2 ust. 1 pkt 1 w. w. ustawy. Postępowanie prowadzone jest zgodnie z procedurami określonymi w Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 zgodnie z zasadą konkurencyjności.

2. Wspólny Słownik Zamówień(CPV):

80000000-4 Usługi edukacyjne i szkoleniowe

80533000-9 Usługi zapoznania użytkownika z obsługą komputera i usługi szkoleniowe

80533100-0 Usługi szkolenia komputerowego

Rozdział. III. Opis Przedmiotu Zamówienia

Firma prowadząca w ramach usługi przeszkoli 2 osoby. Dwa różne szkolenia dla 2 osób. Dla każdej osoby jedno inne szkolenie. Szkolenia muszą mieć inny zakres tematyczny zgodny

z poniżej wymienionymi. **Wykonawca musi dołączyć zakres szkolenia zgodny z OPZ do formularza ofertowego.**

Zamawiający dzieli zamówienie na 2 części:

Część 1 - *Zabezpieczenia w systemie Windows.*

Część 2 - *Szkolenie Bezpieczeństwo sieci.*

Zamawiający daje możliwość złożenia oferty na jedną lub obie części.

Firma prowadząca szkolenie przedstawi oświadczenie, że **funkcjonuje na rynku szkoleń z bezpieczeństwa IT minimum trzy lata**. Jednocześnie **w przeciągu 2 lat przeprowadziła trzy edycje szkoleń** w takiej formie jak podano w specyfikacji, co wykaże w oświadczeniu składanym w załączeniu do formularza ofertowego.

1. Laboratoria i dostęp do platformy szkoleniowej w celu prowadzenia warsztatów zapewnia firma szkoląca.
2. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
3. Czas szkoleń powinien być podzielony na 60% czasu szkolenia ćwiczenia praktyczne a 40% czasu teoria. Szkolenia będą odbywać się w dni robocze.
4. Szkolenia mają odbyć się stacjonarnie. Firma prowadząca zapewni wyżywienie i nocleg.
5. Szkolenia będą prowadzone w języku polskim.

Firma prowadząca zapewni **wydanie zaświadczeń o ukończeniu danego szkolenia Certyfikat ukończenia szkolenia (PDF).**

Wszystkie opracowane materiały muszą zawierać informację o współfinansowaniu i logotypy. Logotypy i informacja o współfinansowaniu muszą być zgodne z wytycznymi: „Podręcznik wnioskodawcy i beneficjenta programów polityki spójności 2014 – 2020 w zakresie informacji i promocji" wydanego przez Ministra Infrastruktury i Rozwoju, zamieszczonego na stronie internetowej www.funduszeeuropejskie.gov.pl.

W przypadku niemożności obsługi zajęć Wykonawca zobowiązuje się powiadomić Zamawiającego na co najmniej 3 dni przed planowanym terminem obsługi zajęć - w zależności od harmonogramu/o przyczynach niemożności wykonania umowy. Musi wskazać nowy termin szkolenia nie przekraczający daty 30.11.2022r.

Wykonawca ma obowiązek przestrzegania zasad równościowych podczas realizacji zamówienia, ze szczególnym uwzględnieniem przekazu równych szans kobiet i mężczyzn, informowania uczestników zajęć o współfinansowaniu projektu ze środków Funduszy Europejskich oraz do umieszczania na wszystkich materiałach logotypów i informacji o współfinansowaniu.

Uczestnicy w trakcie szkolenia wykonują ćwiczenia przy asyście instruktora, który jest do dyspozycji uczestników przez cały czas trwania szkoleń.

Zamawiający zapewni laptop z dowolnym systemem operacyjnym, stabilny internet i słuchawki z mikrofonem.

Szkolenie nr 1. Zabezpieczenia w systemie Windows.

Szkolenie trwa minimum 12 godzin (minimum dwudniowe w godzinach od 9:00 do 16:00), szkolenie warsztatowe, praktyczne szkolenie mające na celu wskazanie problemów z bezpieczeństwem systemów Windows. Teoria i ćwiczenia w celu realnego poznania luk,

błędów. W trakcie zajęć szkolący ma zapewnić pracę na realnych systemach Windows (środowisko testowe zapewnia szkolący). Szczegółowy zakres tematyczny i warsztatowy:

- Architektura systemu Windows w kontekście bezpieczeństwa systemu.
- Działanie omijanie listy kontroli dostępów. Bezpieczeństwo poprzez tokeny i tożsamość obiektów jak przeprowadzić kradzież tokenu. Przywileje systemowe. Konta lokalne.
- Użycie przywilejów systemowych do rozszerzania uprawnień.
- Jak pozyskiwać i wykorzystywać poświadczenia tożsamości z systemu, aplikacji, transmisji sieciowych, domeny, pamięci i inne metody.
- Sposoby szyfrowania w Windows. Praktyczne zastosowania. Rozszyfrowywanie danych bez autoryzacji.
- Wbudowane mechanizmy zdalnego dostępu. Metody dostępu.
- Ataki na procesy działające w systemie Windows.
- Użycie ataków na aplikacje webowe do przejęcia kontroli nad systemem.
- Wykorzystanie PowerShell.
- Bezpieczeństwo domeny Active Directory.
- Bazy danych jako wektor ataku.
- Zacieranie śladów i omijanie typowych zabezpieczeń.

Szkolenie 2. Bezpieczeństwo sieci.

Szkolenie trwa minimum 21godzin (minimum trzydniowe w godzinach od 9:00 do 17:00), szkolenie warsztatowe, mające na celu poznanie metod ochrony sieci komputerowej, zdalnych dostępów do sieci wirtualnych, systemów webowych przed zagrożeniami. Oprócz zajęć teoretycznych, szkolenie ma zapewnić poznanie w praktyce narzędzia, które znacznie ułatwiają realizację testów bezpieczeństwa. W trakcie zajęć szkolący ma zapewnić pracę na realnych systemach, urządzeniach sieciowych, sieciach komputerowych, serwerach. Szczegółowy zakres tematyczny i warsztatowy:

- Zagrożenie współczesnych sieci komputerowych.
- Testy penetracyjne metody, etapy, przykłady zrealizowanych testów, harmonogramy.
- Modyfikacja komunikacji sieciowej.
- Bezpieczeństwo sieci – Ethernet, podsłuchiwanie transmisji, protokołów, ataki.
- Bezpieczeństwo sieci, skanowanie portów urządzeń, podsieci.
- Wykorzystanie wybranych opcji IP do przejmowania topologii sieci.
- Technologie stosowane w zaporach sieciowych. Zasady konfiguracji firewalli, metody skanowania, praktyczne wykrywanie, skanowanie firewalli.
- Bezpieczeństwo wirtualnej sieci prywatnej, skanowanie, łamanie haseł.
- Bezpieczeństwo protokołów sieciowych, praktyczne ćwiczenia modyfikacji komunikacji sieciowej.
- Bezpieczeństwo systemów webowych, testowanie konfiguracji protokołów szyfrowania, ataki na bazy danych, sesje w celu pozyskania dostępu do serwisów.
- Metody ataków na systemy komputerowe z wewnątrz jak i od zewnątrz. Ochrona, tworzenie, testowanie, omijanie systemów wykrywania i zapobiegania włamaniom.
- Podatności błędów programistycznych. Praktyczne ataki na luki w aplikacjach.
- Realizacja przykładowego testu penetracyjnego wykonanego w środowisku testowym zapewnionym przez szkolącego.

Wykaz dokumentów do złożenia przez Wykonawcę:

a) Formularz ofertowy
b) Oświadczenie UWZGLĘDNIAJĄCE PRZESŁANKI WYKLUCZENIA Z ART. 7 UST. 1 USTAWY O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO
c) Oświadczenie o spełnianiu warunków udziału w postępowaniu

Termin realizacji zamówienia: do 30.11.2022r.

Opis sposobu przygotowania ofert:

1) każdy wykonawca może złożyć tylko jedną ofertę,

2) w przypadku złożenia przez dwa lub kilka podmiotów oferty wspólnej (konsorcja), muszą być spełnione następujące warunki:

a) do oferty musi być dołączone pełnomocnictwo /upoważnienie do reprezentowania wykonawców w postępowaniu o udzielenie zamówienia i zawarcia umowy, wystawione zgodnie z wymogami ustawowymi i podpisane przez prawnie upoważnionych przedstawicieli każdego z partnerów,

b) oferta winna być podpisana przez każdego partnera lub ustanowionego pełnomocnika,

c) ustanowiony pełnomocnik winien być upoważniony do zaciągania zobowiązań i płatności w imieniu każdego partnera, na rzecz każdego z partnerów oraz do wyłącznego występowania w realizacji kontraktu.

3) oferta, na której Wykonawca nie złoży podpisu pod zgodą na przetwarzanie danych osobowych na potrzeby niniejszego postępowania, będzie odrzucona.

Zamawiający daje możliwość złożenia oferty na jedną lub obie części.

Do udziału w postępowaniu dopuszczeni są Oferenci, którzy posiadają dobrą sytuację ekonomiczną i finansową spełniający łącznie następujące warunki:

1. Znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
2. Nie są przedmiotem wszczętego postępowania upadłościowego ani jego upadłość nie jest ogłoszona, nie jest poddany procesowi likwidacyjnemu, a jego sprawy nie są objęte zarządzeniem komisarycznym lub sądowym.
3. Urzędujący członkowie organów/ wspólnicy oferenta nie zostali prawomocnie skazani 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.

Miejsce oraz termin składania ofert:

1) Ofertę na FORMULARZU OFERTY wraz z załącznikami należy złożyć w nieprzekraczalnym terminie **do dnia 06.10.2022 r.** do godz. 10:00 wyłącznie w formie elektronicznej na adres: piotr.tomaszewski@mlawa.pl , wskazane jest aby FORMULARZ OFERTY (wraz z załącznikami) był załącznikiem do e-maila.

2) Wykonawca może, przed upływem terminu do składania ofert, zmienić lub wycofać ofertę.

Kryteria oceny ofert:

Cena ofertowa – 100%

W trakcie oceny każdej ofercie przyznane zostaną punkty dla kryterium cena, według wzoru:

$$C=(C_{min} / C_{oferta}) \times 100 \text{ pkt.}$$

gdzie:

C_{min} oznacza najniższą cenę zaoferowaną w postępowaniu,

C_{oferta} oznacza cenę badanej oferty.

Sposób oceny: za najkorzystniejszą zostanie wybrana oferta, która zgodnie z powyższymi kryteriami oceny ofert uzyska najwyższą liczbę punktów spośród ofert nie podlegających odrzuceniu.

Warunki umowy:

1) Umowa w sprawie realizacji zamówienia publicznego zawarta zostanie z uwzględnieniem postanowień wynikających z treści niniejszej oferty wraz z załącznikami.
2) Zamawiający podpisze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę.
3) Zamawiający zastrzega sobie prawo zmian treści umowy po jej podpisaniu. Zmiany te mogą dotyczyć w szczególności:
   a) wystąpienia uzasadnionych zmian w zakresie i sposobie wykonania przedmiotu zamówienia;
   b) wystąpienia obiektywnych przyczyn niezależnych od Zamawiającego i Wykonawcy;
   c) wystąpienia okoliczności będących wynikiem działania siły wyższej;
   d) zmiany istotnych regulacji prawnych;
   e) zmian w zawartej umowie o dofinansowanie;
   f) gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy;
   g) wynikną rozbieżności lub niejasności w Umowie, których nie można usunąć w inny sposób, a zmiana Umowy będzie umożliwiać usunięcie rozbieżności i doprecyzowanie Umowy w celu jednoznacznej interpretacji jej zapisów przez Strony.
   h) wzór umowy został załączony do postępowania

Piotr Tomaszewski; UM Mława

Elektronicznie podpisany przez Piotr Tomaszewski; UM Mława
Data: 2022.09.27 09:26:21 +02'00'