IB.271.3.2022

Opis przedmiotu zamówienia:

1. Przedmiot zamówienia:

Diagnoza cybezpieczeństwa

1. Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa – Urzędu Miejskiego w Bolkowie.
2. Diagnoza musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa" stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina (załącznik nr 3 do zapytania – diagnoza)
3. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
4. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 2, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w pkt. 3.
5. Jednostki samorządu terytorialnego biorące udział w projekcie „Cyfrowa Gmina" są zobowiązane do przeprowadzenia diagnozy cyberbezpieczeństwa będącej przedmiotem niniejszego zamówienia. Niezwłocznie po jej przeprowadzeniu, jej wyniki mają być przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednosteksamorządowych. Wykonawca jest zobowiązany mieć na uwadze powyższy cel przeprowadzenia diagnozy i jej przeznaczenia.

Szkolenia

Wykonawca przeprowadzi szkolenia z cyberbezpieczeństwa dla pracowników Urzędu Miejskiego w Bolkowie oraz Zakładu Gospodarki Komunalnej Bolkowie.

Wymagania ogólne dla szkoleń:

1. Planowany czas trwania zajęć ok. 2,5 godziny zegarowe na każdą grupę,
2. W ramach usługi zostanie przeszkolonych ok. 48 osób.
3. Ze względu na konieczność zachowania ciągłości pracy obu jednostek szkolenia zostaną przeprowadzone w grupach. Planowy jest podział na 4 grupy szkoleniowe.
4. Termin planowanych szkoleń - po przeprowadzeniu diagnozy ceyberbezpieczeństwa.
5. Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
6. Zamawiający dopuszcza przeprowadzenie szkolenia przez wideokonferencję.

Ramowy zakres szkolenia:

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2. Polityka bezpieczeństwa w organizacji.
3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.
4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
5. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko".

6. bezpieczeństwo stacji roboczych (komputery użytkownika).
7. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
8. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
9. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
10. Prawidłowe korzystanie z oprogramowania antywirusowego.
11. Zasady aktualizacji programów i aplikacji.
12. Szyfrowanie dokumentów i poczty elektronicznej.
13. Polityka haseł, zarządzanie dostępem i tożsamością.
14. Bezpieczeństwo sieci LAN i Wi-Fi.
15. Bezpieczeństwo aplikacji ministerialnych oraz wewnątrzorganizacyjnych.
16. Bezpieczeństwo stacji roboczych (komputery użytkownika).
17. Zarządzanie tożsamością w internecie oraz wewnątrz organizacji.
18. Bezpieczeństwo baz danych i infrastruktury.
19. Bezpieczeństwo mobilne.
20. Odpowiednie zabezpieczenie techniczne sieci.
21. Optymalna architektura systemowo-serwerowa.
22. Techniki socjotechniki (inżynieria społeczna).
23. Bezpieczeństwo sieci LAN i Wi-Fi.
24. Zarządzanie tożsamością w internecie oraz wewnątrz organizacji.
25. Bezpieczeństwo baz danych i infrastruktury.
26. Odzyskiwanie po awarii – planowanie ciągłości działania.
27. Optymalna architektura systemowo-serwerowa.

2. Warunki udziału w postępowaniu

O udzielenie niniejszego zamówienia mogą ubiegać się wykonawcy, którzy spełniają poniższe warunki:

1. Diagnoza musi być przeprowadzona przez osobę **posiadającą certyfikat uprawniający do przeprowadzenia audytu,** o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
2. W celu potwierdzenia wymaganych wyżej warunków wraz z ofertą należy dostarczyć dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu wymienione w pkt 2 ust 1.
3. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
4. Do udziału w postępowaniu dopuszczeni są jedynie Wykonawcy, którzy nie są powiązani z Zamawiającym osobowo lub kapitałowo. Przez powiązania osobowe lub kapitałowe rozumie się wzajemne powiązania między beneficjentem (Zamawiającym) lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związanych z przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:
    a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
    b) posiadaniu co najmniej 10 % udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony w wytycznych programowych,

c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Weryfikacja nastąpi w oparciu o oświadczenie Wykonawcy o braku w/w powiązań osobowych lub kapitałowych z Zamawiającym – załącznik nr 3.
W sytuacji wystąpienia powiązania, o którym mowa w pkt. 4 Wykonawca będzie podlegał wykluczeniu z postępowania.

5. Podstawy wykluczenia Wykonawcy z udziału w postępowaniu. Zamawiający wykluczy z udziału w postępowaniu Wykonawcę, który:
   a) w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd Zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez Zamawiającego w postępowaniu o udzielenie zamówienia,
   b) bezprawnie wpływał lub próbował wpłynąć na czynności Zamawiającego lub pozyskać poufne informacje, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia,
   c) z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych,
   d) w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych,

   Weryfikacja nastąpi w oparciu o oświadczenie Wykonawcy o braku podstaw do wykluczenia – załącznik nr 4.

Osoba uprawniona do porozumiewania się z Wykonawcą

Osobą uprawnioną do porozumiewania się z Wykonawcami jest:
Rafał Bonna – inspektor ds. informatyki Urzędu Miejskiego w Bolkowie, Rynek 1, 59-420 Bolków, tel. 75 74 13 215 wew. 313, email: informatyk@bolkow.pl

Zawartość oferty

Wykonawca powinien dostarczyć następujące dokumenty:
a) Ofertę cenową przygotowaną zgodnie ze wzorem stanowiącym załącznik nr 2, z podaniem ceny ryczałtowej powiększonej o należny podatek VAT,
b) Oświadczenie – załącznik nr 3
c) Oświadczenie – załącznik nr 4
d) Oświadczenie – załącznik nr 5
e) Dokument potwierdzający posiadanie certyfikatu uprawniającego do przeprowadzenia audytu

Oferty, w skład których nie będą wchodzić wszystkie załączniki zostaną odrzucone.

Oferta, aby była ważna, musi być podpisana przez upoważnionych przedstawicieli Wykonawcy, wymienionych w aktualnych dokumentach rejestracyjnych firmy lub przez osoby posiadające pisemne pełnomocnictwo. Wyżej wskazane pełnomocnictwo należy dołączyć do oferty.

Postanowienia końcowe

Zamawiający informuje Wykonawców, że nie przysługują im środki ochrony prawnej, określone ustawą Prawo zamówień publicznych. Niniejsze postępowanie nie jest prowadzone na podstawie ustawy z 11 września 2019 r. Prawo zamówień publicznych, w związku z tym procedury nie przewidują możliwości składania protestu, odwołania lub skargi w odniesieniu do prowadzonej przez Inwestora procedury wyboru wykonawcy danej usługi.

Zamawiający zastrzega sobie prawo do:

- swobodnego wyboru ofert w ramach kryteriów określonych powyżej lub uznania, że postępowanie nie dało rezultatu,
- odwołania postępowania, unieważnienia go w całości lub części w każdym czasie,
- zamknięcia postępowania bez dokonania wyboru oferty,
- zmiany terminów wyznaczonych w ogłoszeniu,
- żądania szczegółowych informacji i wyjaśnień od Wykonawców na każdym etapie postępowania,
- Wyłącznej interpretacji zapisów ogłoszenia, jak również jego załączników.

Okres związania ofertą: 30 dni od daty terminu składania ofert.