

ZAPYTANIE OFERTOWE na "Przeprowadzenie audytu zgodności z KRI oraz audytu penetracyjnego"



Gmina Ozimek realizuje projekt „e-Ozimek rozwój cyfrowych usług” dofinansowany z Funduszy Europejskich, z Regionalnego Programu Operacyjnego Województwa Opolskiego na lata 2014-2020 współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego.

03.12.2018 r. Dodano ogłoszenie o wynikach zapytania ofertowego

03.12.2018 r. Dodano informację z otwarcia ofert zapytania ofertowego

ZAPYTANIE OFERTOWE

„Przeprowadzenie audytu zgodności z KRI oraz audytu penetracyjnego”

Ozimek, 22 listopada 2018r.

Szanowni Państwo,

I. Zaproszenie

Burmistrz Ozimka zaprasza do złożenia oferty cenowej na usługę przeprowadzenia audytu zgodności z KRI oraz audytu penetracyjnego. Audyt ma na celu ustalenie aktualnego stanu całego systemu informatycznego Zamawiającego. Wykrycie potencjalnych zagrożeń i nieprawidłowości oraz ocenę bezpieczeństwa przetwarzania danych, ze szczególnym uwzględnieniem przetwarzania danych osobowych i zgodności z aktualnie obowiązującymi aktami prawnymi. Audyt powinien być przeprowadzony najnowocześniejszymi narzędziami i zgodnie z metodologią, która gwarantuje rzetelność oceny bieżącego stanu bezpieczeństwa systemów informatycznych, zgodnie z poniższymi założeniami:

II. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu audytu zgodności z KRI oraz audytu penetracyjnego zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017, poz. 2247).

Wykonawca przed przystąpieniem do realizacji audytu jest zobowiązany do podpisania klauzuli poufności i jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni dotyczących Zamawiającego, a w szczególności danych osobowych, technicznych, ekonomicznych lub organizacyjnych.

Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy

w trakcie realizacji zadań audytowych i jest bezterminowe.

1. Obszary kontroli:

2. Legalność oprogramowania i komputerów
3. Audyt penetracyjny.

III.1. W zakresie legalności oprogramowania i komputerów:

- Uporządkowanie dokumentacji licencyjnej,
- Skanowanie komputerów przez Audytora,
- Oględziny stanowisk pracy,
- Sporządzenie rejestru dokumentacji licencyjnej,
- Usługi aktualizacji oprogramowania,
- Opracowanie raportu wstępnego,
- Opracowanie wymagań dotyczących likwidacji niezgodności -plan naprawczy,
- Wdrożenie procedur przenoszących odpowiedzialność za zainstalowane oprogramowanie na użytkownika końcowego wg zaleceń BSA (Business Software Alliance),
- Wykonanie końcowego skanowania komputerów,
- Przygotowanie raportu końcowego.

III. 2. W zakresie audytu penetracyjnego:

- Analiza posiadanych systemów operacyjnych i oprogramowania oraz ustalenie na jakiego typu zagrożenia są podatne,
- Rozpoznanie środowiska (serwisy www, bazy RIPE, serwery DNS, nagłówki SMTP, wyszukiwarki internetowe, portale-intranet, itp.,
- Analiza konfiguracji systemów, aplikacji (w tym baz danych) i urządzeń pod kątem zalecanych praktyk dotyczących bezpieczeństwa,
- Wyszukanie zagrożeń związanych z posiadanymi systemami i wersjami oprogramowania w bazach powszechnie znanych luk i exploitów (CVE),
- Skanowanie niezależnymi narzędziami dedykowanymi dla różnych systemów operacyjnych,
- Skanowanie puli adresowych IP (icmp scan, tcp scan),

- Skanowanie portów TCP/UDP różnymi metodami (Xmas, connect, Null, SYN, FIN),
- Analiza ruchu w sieci lokalnej na poziomie wszystkich warstw modelu ISO/OSI (m.in. protokoły Ethernet, IP, TCP/UDP, DNS, DHCP, RDP, MTP, POP3, IMAP, FTP, HTTP...);
- Próby przekierowania ruchu z wykorzystaniem techniki zatruwania tablicy ARP oraz protokołu ICMP;
- Próby przejęcia kontroli nad elementami infrastruktury (urządzenia aktywne sieci, urządzenia zaplecza technicznego, kamery, kontrola dostępu, UPS-y, monitoring środowiskowy, panele administracyjne, urządzenia pamięci masowych i backupu, kontrolery zdalnego zarządzania serwerami),
- Ocena ryzyka związanego ze stwierdzonymi lukami,
- Opracowanie zaleceń naprawczych i podnoszących poziom bezpieczeństwa,
- Przygotowanie raportu dotyczącego braków, potencjalnych luk oraz wskazanie poprawek, packów i wersji oprogramowania likwidujących potencjalne zagrożenia,

W ramach prac Wykonawca zidentyfikuje występujące problemy i ich przyczyny, opracuje rekomendacje działań i koniecznych zmian odnoszących się do zapewnienia zgodności działania Zamawiającego z wymaganiami KRI.

1. Wymagane rezultaty audytu

Wykonawca sporządzi sprawozdanie audytowe, które będzie zawierać:

1. Szczegółowy opis i ocenę stanu wszystkich obszarów podlegających audytowi.
2. Wykaz wszystkich problemów oraz wynikających z tego ryzyk wraz z oceną ryzyka wystąpienia wykrytych zagrożeń.
3. Zobrazowanie połączeń logicznych, sieci lokalnej oraz styku sieci lokalnej z siecią Internet, z uwzględnieniem wszystkich urządzeń ich adresacji i działających usług, używanych portów i protokołów.
4. Szczegółową, elektroniczną inwentaryzację sprzętu i oprogramowania działającego w infrastrukturze informatycznej Zamawiającego.
5. Zalecenia dotyczących sposobów, metod i środków usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyk. Lista poprawek do zainstalowania oraz szczegółowy opis zalecanych zmian konfiguracji.

Wszystkie dokumenty związane z przeprowadzonym audytem Wykonawca dostarczy Zamawiającemu w postaci wydruku w dwóch egzemplarzach i w postaci elektronicznej.

Wykonawca pisemnie zobowiąże się, że dokumenty te będzie traktował jako poufne i nie przekaze ani nie udostępni ich nikomu bez pisemnej zgody Zamawiającego.

Wykonawca, z dniem zatwierdzenia przez Zamawiającego sprawozdania audytowego, przeniesie na Zamawiającego autorskie prawa majątkowe do sprawozdania audytowego na polach eksploatacji, obejmujących:

- odtwarzanie,
- utrwalanie i trwałe zwielokrotnianie całości lub części utworu, wszystkimi znanymi w chwili zawierania Umowy technikami, w tym techniką drukarską, reprograficzną, zapisu

- magnetycznego oraz techniką cyfrową,
- przekazywanie,
- przechowywanie,
- wyświetlanie,
- wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji,
- tłumaczenie,
- przystosowywanie,
- zmiany układu lub jakiegokolwiek inne zmiany.

V. Warunki udziału w postępowaniu

1. Wiedza i doświadczenie:

Zamawiający uzna, że Wykonawca spełnia warunek wiedzy i doświadczenia, gdy Wykonawca w okresie ostatnich trzech lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie) wykonał lub wykonuje co najmniej dwie usługi odpowiadające swoim rodzajem usługom stanowiącym przedmiot zamówienia.

Na potwierdzenie spełnienia warunku w zakresie wiedzy i doświadczenia Wykonawca zobowiązany jest przedłożyć wykaz usług, zgodnie z wzorem stanowiącym załącznik nr 2 do zapytania ofertowego. Wykonanie lub wykonywanie usług zamieszczonych w wykazie musi być potwierdzone poświadczonymi za zgodność z oryginałem referencjami, że usługi te zostały wykonane należyście.

VI. Informacje dotyczące warunków składania ofert:

Ofertę cenową na Formularzu ofertowym należy złożyć w terminie do **dnia 27 listopada 2018 r. do godz. 10:00**, drogą elektroniczną – skan podpisanej oferty wraz załącznikami – na adres: sekretarz @ugim.ozimek.pl, w tytule maila proszę wpisać: „Przeprowadzenie audytu zgodności z KRI oraz audytu penetracyjnego”

Miejsce świadczenia usługi: siedziba Zamawiającego w Ozimku.

Oferta powinna zawierać:

1. Formularz ofertowy, zgodnie ze wzorem stanowiącym **Załącznik nr 1** do zapytania ofertowego.
2. Wykaz usług zrealizowanych przez Wykonawcę, zgodnie ze wzorem stanowiącym **Załącznik nr 2** do zapytania ofertowego.
3. Aktualny odpis z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej.

VII. Kryteria oceny ofert

1. Zamawiający dokona wyboru oferty biorąc pod uwagę cenę oferty oraz wskazany termin realizacji zamówienia.
2. Oferta Wykonawcy może uzyskać maksymalnie 100 punktów. Przy dokonywaniu wyboru najkorzystniejszej oferty Zamawiający posługiwać się będzie kryterium:

• „Cena” - waga 100% (maksymalnie 100 punktów)

Ocena złożonych ofert w zakresie kryterium „Cena” zostanie dokonana na podstawie podanej w ofercie przez Wykonawcę całkowitej ceny brutto za realizację usługi będącej przedmiotem niniejszego zamówienia.

Liczba punktów w tym kryterium zostanie obliczona wg następującego wzoru:

$$C_n$$

$$C_{of} = \frac{C_n}{C_{bo}} \times 100 \text{ pkt}$$

$$C_{bo}$$

Gdzie:

C_{of} = liczba punktów za kryterium cena

C_n = najniższa cena ofertowa brutto spośród badanych ofert

C_{bo} = cena brutto oferty badanej

3. Zamawiający udzieli zamówienia temu Wykonawcy, który nie zostanie wykluczony, a jego oferta nie zostanie odrzucona i uzyska największą liczbę punktów.
4. W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Wykonawcami, w celu uzupełnienia lub wyjaśnienia treści ofert.

VIII. Informacje dodatkowe:

1. Zamawiający informuje, że usługi stanowiące przedmiot niniejszego zamówienia są dofinansowane z Funduszy Europejskich, z Regionalnego Programu Operacyjnego Województwa Opolskiego na lata 2014-2020 współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego.
2. Cena oferty musi zawierać wszystkie koszty i opłaty niezbędne dla realizacji zamówienia.

3. Wykonawca ma prawo złożyć tylko jedną ofertę. Złożenie przez tego samego Wykonawcę więcej niż jednej oferty, w sposób inny niż określony w pkt. VI lub po terminie, spowoduje jej odrzucenie.
4. Niespełnienie warunków udziału oraz nie przedłożenie dokumentów wymaganych na ich potwierdzenie skutkować będzie wykluczeniem Wykonawcy (a jego oferta zostanie wówczas odrzucona).
5. Z wyłonionym Wykonawcą zostanie zawarta pisemna umowa, zgodnie z Istotnymi Postanowieniami Umowy, stanowiącymi **Załącznik nr 3** do zapytania ofertowego.

6. Warunku płatności:

Zamawiający dokonuje płatności na podstawie dokumentów księgowych, wystawionych z co najmniej 14-dniowym terminem płatności liczonym od daty wpływu do siedziby Zamawiającego prawidłowo wystawionego dokumentu księgowego. Podstawę do wystawienia faktury VAT stanowi podpisany bez uwag przez Strony protokół odbioru.

Faktura / rachunek* obejmować będzie zapłatę za należyte zorganizowanie i przeprowadzenie szkolenia.

7. Pozostałe warunki dotyczące realizacji zamówienia zostały określone w Istotnych Postanowieniach Umowy.
8. Zamawiający zastrzega sobie prawo do unieważnienia przedmiotowego zapytania ofertowego na każdym jego etapie, bez podania przyczyny.