Pasłęk 18.11.2020 r.

Zapytanie o cenę

W związku z zamiarem opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zgodną ISO/IEC 27001 w Urzędzie Miejskim w Pasłęku, zapraszamy do składania ofert na ww. usługę.

1. Cel zamówienia

Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Urzędu poprzez opracowanie uregulowań w zakresie bezpieczeństwa informacji poprzez zaprojektowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, w tym Polityki Bezpieczeństwa Informacji, zgodnie z wymaganiami nw. aktów prawnych, norm i wytycznych:

- ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (w skrócie „KRI");
- ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
- Polskiej normy PN-EN ISO/IEC 27001:2017-06 wyłącznie w ograniczonych przez Zamawiającego obszarach wymienionych w pkt II. 3. a;
- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), w skrócie „RODO";
- ustawa o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781)

2. Realizacja zamówienia

Realizacja zamówienia ma spowodować następujące skutki:

- zapewnić bezpieczeństwo danych i systemów posiadanych przez Urząd oraz powierzanych Urzędowi w oparciu o akty prawne i wytyczne wymienione w pkt 1,
- ograniczyć czas niedostępności systemów informatycznych Urzędu z powodów ich awarii, poprzez opracowanie Planów Ciągłości Działania,
- zoptymalizować koszty utrzymania i rozwoju systemów informatycznych oraz koszty zabezpieczenia infrastruktury teleinformatycznej Urzędu przed działaniem szkodliwego oprogramowania i próbami włamań;
- zapewnić bezpieczeństwo procesu udostępniania danych.

3. Opis i zakres przedmiotu zamówienia.

1. Podstawowe wymagania w zakresie zaprojektowania dokumentów, procedur i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, w tym Polityki Bezpieczeństwa Informacji:

a) Usługa zaprojektowania dokumentów, procedur i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (w skrócie SZBI) w tym Polityki Bezpieczeństwa Informacji (w skrócie PBI) będzie obejmować swoim zakresem:
   - Etap I - Audyt przedwdrożeniowy w Urzędzie;
   - Etap II - Szkolenie zespołu Wdrożeniowego
   - Etap III - Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Urzędzie
   - Etap IV - Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji
   - Etap V - Wdrożenie SZBI

b) Każdy etap określony w pkt 3. 1. a) podlega ocenie oraz formalnemu zaakceptowaniu przez Zamawiającego.

c) Wszelkie informacje dotyczące usługi przekazywane między Wykonawcą a Zamawiającym będą zabezpieczone przed nieuprawnionym dostępem w sposób określony przez Zamawiającego.

Etap I - Audyt przedwdrożeniowy

a) Audyt przedwdrożeniowy ma na celu weryfikację poziomu spełnienia wymagań określonych w

rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Krajowych Ram Interoperacyjności oraz wybranych elementów normy PN-EN ISO/IEC 27001:2017-06 przez Urząd, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych w Urzędzie, w obszarach określonych załącznikiem A do ww. normy, tj.:

- Polityki bezpieczeństwa informacji,
- Organizacja bezpieczeństwa informacji,
- Bezpieczeństwo zasobów ludzkich
- Zarządzanie aktywami,
- Kontrola dostępu,
- Kryptografia,
- Bezpieczeństwo fizyczne i środowiskowe,
- Bezpieczna eksploatacja,
- Bezpieczeństwo komunikacji,
- Pozyskiwanie, rozwój i utrzymanie systemów,
- Relacje z dostawcami,
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania.

Etap II - Szkolenie zespołu Wdrożeniowego

Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkolenia z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji dla zespołu wdrożeniowego składającego się wyznaczonych pracowników Urzędu.

Celem szkolenia dla liderów SZBI jest przygotowanie do realizacji projektu w Urzędzie.

Etap III - Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Urzędzie

W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Urzędzie, a w szczególności:

- opracować metodykę szacowania ryzyka spełniającą wymagania Krajowych Ramach Interoperacyjności, norm ISO/IEC 27001:2017-06, PN-ISO/IEC 27005:2014, optymalną ze względu na charakter działalności Urzędu;
- opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
- przeszkolić wybranych pracowników Urzędu w zakresie przyjętej metodyki szacowania ryzyka;
- przeprowadzić wspólnie z wyznaczonymi pracownikami Urzędu proces szacowania ryzyka, w tym: zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
- opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Urzędu;
- opracować przy współudziale wyznaczonych pracowników Urzędu plan postępowania z ryzykiem.

Dokumentację, o której mowa w etapie III , tj. metodykę szacowania ryzyka, raport z procesu szacowania ryzyka oraz plan postępowania z ryzykiem Wykonawca przekaże Zamawiającemu w w formie elektronicznej w pliku edytowalnym w formatach: docx lub xlsx. Dokumentację w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na nośniku danych, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.

Etap IV - Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji

a) Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest zaproponować organizację Systemu Zarządzania Bezpieczeństwem Informacji oraz opracować i przedstawić koncepcję treści i wdrożenia Polityki Bezpieczeństwa Informacji w Urzędzie.
b) Koncepcja będzie w szczególności zawierać mapę dokumentów, stanowiącą szczegółowy wykaz dokumentów z zaznaczeniem ich wzajemnych powiązań, w tym:
    - dokument główny, Polityka Bezpieczeństwa Informacji, definiujący m.in. jej cele, zakres,

wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;
- Polityki dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w Urzędzie w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk;
- Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

c) Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia SZBI i PBI.
d) Na podstawie zatwierdzonej przez Zamawiającego koncepcji, o której mowa w etap IV a) i b), Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty muszą być zgodne ze wszystkimi wymaganiami prawnymi, którymi podlega Urząd.
e) Wszystkie dokumenty Wykonawca przekaże Zamawiającemu w formie elektronicznej w plikach edytowalnych w formatach: docx lub xlsx. Dokumentację w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na nośniku danych, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.
f) Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

Etap V - Wdrożenie SZBI

Wykonawca zobowiązany jest do:
- Przygotowanie materiałów szkoleniowych dla pracowników i Audytorów Wewnętrznych SZBI,
- Przeprowadzenie szkolenia dla Audytorów Wewnętrznych SZBI,
- Przeprowadzenie szkolenia dla kluczowych pracowników z wdrażanych mechanizmów organizacyjnych oraz podstawowych zasad ochrony informacji,
- Wsparcie przy przeprowadzeniu audytu wewnętrznego,
- Wsparcie przy przeprowadzeniu przeglądu zarządzania.

a) Szkolenia dla wszystkich ww. grup będą odbywały się w siedzibie Zamawiającego, lub za pomocą wideokonferencji, w dni robocze w godzinach 8:30-15:30.
b) Wykonawca przekaże do akceptacji Zamawiającemu harmonogram szkoleń, materiały szkoleniowe i prezentacje najpóźniej na 14 dni przed planowanym terminem rozpoczęcia szkoleń.
c) Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę materiałów szkoleniowych i harmonogramu szkoleń, w tym do zmiany planowanych terminów szkoleń. Wykonawca zobowiązany jest do uwzględnienia uwag wniesionych przez Zamawiającego.
d) Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu:
    - imiennej listy obecności uczestników szkolenia sporządzanej odrębnie dla każdego dnia szkolenia, zawierającej: informacje o liczbie godzin, obecności danej osoby, podpis uczestnika szkolenia, podpis wykładowcy/-ów;
    - ankiet oceny szkolenia wypełnionych i podpisanych przez uczestników szkolenia.

Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń.

4. Termin wykonania zadania:

4.1. Rozpoczęcie zadania: po otrzymaniu i przyjęciu warunków zlecenia
4.2. Zakończenie zadania: do dnia 20 czerwca 2021 r.

5. Wymagania.

O udzielenie zamówienia mogą ubiegać się wykonawcy posiadający wiedzę i doświadczenie zawodowe umożliwiające wykonanie przedmiotu zamówienia tj. zrealizowali minimum 3 zadania ww. zakresie.

Warunkiem przyjęcia oferty jest przedstawienie przynajmniej 3 referencji dotyczących opracowania i wdrożenia SZBI w przeciągu ostatnich 5 lat (w tym jedną w przeciągu ostatnich 3 lat).

6. Sposób przygotowania oferty.

Oferty należy składać na formularzu stanowiącym załącznik nr 1 do niniejszego zaproszenia.

Do wypełnionego formularza należy dołączyć:

- Oświadczenie stanowiące załącznik nr 2 do niniejszego zaproszenia.
- 3 referencje potwierdzające należyte wykonanie usługi zgodnie z pkt. 5 niniejszego zaproszenia.

7. Miejsce i termin składania ofert.

Ofertę należy złożyć w sekretariacie Urzędu Miejskiego w Pasłęku, Pl. Św. Wojciecha 5, 14-400 Pasłęk, lub przesłać pocztą w terminie do dnia 25 listopada 2020 r. do godziny 14:00 (liczy się data wpływu do urzędu).

Ofertę należy złożyć w zamkniętej kopercie opatrzonej podpisem „Oferta na wykonanie zadania pn. „Usługa opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001 w Urzędzie Miejskim w Pasłęku", nie otwierać przed dniem 27.11.2020 r. do godz. 10:15

Otwarcie ofert nastąpi w dniu 27 listopada 2020 r. o godz. 10:15.

8. Kryteria wyboru oferty: najniższa cena

9. Informacja o wyborze oferty zostanie umieszczona w Biuletynie Informacji Publicznej Urzędu Miejskiego w Pasłęku – http://bip.paslek.pl.

Załącznik nr 1
do zapytania

…....
(miejscowość i data)

FORMULARZ OFERTY
na wykonanie zamówienia publicznego o wartości netto poniżej 30 000 €.

I. Nazwa i adres ZAMAWIAJĄCEGO:

Gmina Pasłęk - Urząd Miejski w Pasłęku
Plac Św. Wojciecha 5, 14-400 Pasłęk

II. Nazwa przedmiotu zamówienia:

Usługa opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zgodną ISO/IEC 27001 w Urzędzie Miejskim w Pasłęku.

III. Tryb postępowania: Zapytanie ofertowe.

IV. Nazwa i adres WYKONAWCY

.....
.....
Tel .....
Fax .....
Regon.....
NIP .....
KRS .....

1. Oferuję wykonanie przedmiotu zamówienia za:
Wartość umowy..... zł netto + ... zł (……..%)VAT
= ..... zł brutto
Słownie……
…… zł brutto.

2. Deklaruję ponadto:
   a) termin wykonania usługi …… m-cy od dnia podpisania umowy.
   b) warunki płatności: ……
   c) udzielenie gwarancji Zamawiającemu na warunkach przedstawionych w zaproszeniu
   d) spełnienie wymagań dla usług wymienionych w szczegółowej specyfikacji dla projektów ISO/IEC 27001

   e) inne .....,

…....
(podpis osoby uprawnionej
do składania oświadczeń woli
w imieniu Wykonawcy)

Załącznik nr 2
do zapytania

OŚWIADCZENIE

Składając ofertę w trybie uproszczonym (pozaustawowe) na: Usługę opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001 w Urzędzie Miejskim w Pasłęku

oświadczamy, że spełniamy warunki dotyczące:

1. posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2. posiadania wiedzy i doświadczenia;
3. spełniamy wymagania zawarte w normie ISO 10019
4. dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
5. sytuacji ekonomicznej i finansowej

.....
(podpis osoby uprawnionej
do składania oświadczeń woli
w imieniu Wykonawcy)