ABI.142.1.2017 **Kobyłka, dnia 6 grudnia 2017 r.**

REGULAMIN
konkursu ofert
na wykonanie usługi audytu bezpieczeństwa informacji
wraz z wdrożeniem RODO
w Urzędzie Miasta Kobyłka

wartość zamówienia nie przekracza kwoty 30 000 Euro

I. ZAMAWIAJĄCY

Miasto Kobyłka
ul. Wołomińska 1
05-230 Kobyłka
NIP: 125-133-23-90, REGON: 013269663,
tel. 22 760-70-54 Administrator Bezpieczeństwa Informacji Wojciech Reutt
e-mail: urzad@kobylka.pl wojciech.reutt@kobylka.pl
strona: www.kobylka.pl www.bip.kobylka.pl

II. PROCEDURA

Zamawiający prowadzi postępowanie w trybie konkursu ofert – art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164) (wartość zamówienia nie przekracza kwoty 30 000 Euro).

III. PRZEDMIOT ZAMÓWIENIA

Zamawiający oszacował przedmiot zamówienia na ok. 30 000,00 zł z VAT.

Przedmiotem zamówienia jest audyt bezpieczeństwa informacji (zwłaszcza danych osobowych i bezpieczeństwa teleinformatycznego) w Urzędzie Miasta Kobyłka w tym wdrożenie niezbędnych dokumentów, procesów i procedur wymaganych w RODO oraz wdrożenie niezbędnych dokumentów i procedur wymaganych w RODO w jednostkach podległych (Biblioteka Publiczna, Miejski Ośrodek Kultury, Ośrodek Sportu i Rekreacji).
Szczegółowy, minimalny zakres przedmiotu zamówienia stanowi załącznik nr 1 do niniejszego regulaminu. Wykonawca może zaproponować poszerzenie zakresu zamówienia (w ramach kryterium pozacenowego).
Zamawiający oczekuje wykonanie całości przedmiotu zamówienia bezpośrednio przez wykonawcę (brak podwykonawców). Jedyny zakres, który zamawiający przewiduje, jako możliwy do powierzenia podwykonawcom to szkolenia dla pracowników na zakończenie audytu.

IV. TERMIN WYKONANIA ZAMÓWIENIA

Umowa będzie podpisana nie wcześniej niż 02.01.2018 r.
Wykonawca zrealizuje przedmiot zamówienia (w tym ew. oferowane poszerzenia) do 30.04.2018 r. (płatności etapowo – Zamawiający zakłada płatności: etap audytu danych osobowych ok. 20% ceny oferty, etap audytu bezpieczeństwa teleinformatycznego ok. 30% ceny oferty, szkolenie ok. 5% ceny oferty, inne ew. etapy łącznie ok. 15% ceny oferty, pozostałą część wynagrodzenia po zrealizowaniu całości) wg harmonogramu rzeczowo-finansowego ustalonego w ofercie a uszczegółowionego w ramach formalności przed podpisaniem umowy.

V. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają następujące warunki udziału w postępowaniu:
   1) posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
   2) posiadają wiedzę i doświadczenie w przedmiocie zamówienia;
   3) dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
   4) znajdują się w sytuacji ekonomicznej i finansowej umożliwiającej realizację przedmiotu zamówienia.
2. Sposób dokonywania oceny spełniania warunków udziału w postępowaniu:
   1) w celu spełnienia warunku wymienionego w ust. 1 pkt 2 wykonawca winien wykazać wykonanie w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, usług w zakresie wykonania audytów, łącznie (wyłącznie doświadczenie własne wykonawcy – uniemożliwia się użyczanie wiedzy i doświadczenia od podmiotu trzeciego):
      a) audyty danych osobowych w:
         — co najmniej 4 urzędach gminy/miasta o liczbie mieszkańców min. 20 tys. lub w urzędach powiatowych lub urzędach administracji rządowej terenowej na poziomie powiatu (administracji zespolonej lub niezespolonej) – łącznie co najmniej 4 takie podmioty,

      Zamawiający uzna za równoważny z powyższym wymogiem audyt w co najmniej 1 urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub oddziale wojewódzkim takiego urzędu lub sądzie lub ambasadzie lub innym centralnym organie państwowym lub jego oddziale wojewódzkim lub aktualnym urzędzie wojewódzkim lub marszałkowskim lub ich jednostkach podległych lub urzędzie administracji rządowej terenowej na poziomie województwa (administracji zespolonej lub niezespolonej) lub urzędzie miejskim aktualnego miasta wojewódzkiego lub uczelni wyższej (mającej status uczelni akademickiej) lub państwowej jednostce badawczej.
      b) audyty bezpieczeństwa teleinformatycznego łącznie w:
         — co najmniej 4 podmiotach wymienionych w lit. a

      Równoważność, jak w lit. a. Może być doświadczenie z lit. a. (audyt, który obejmował oba zakresy).

      Wykonawca w kryterium oceny ofert może wykazać usługi wykazane w warunku wiedzy i doświadczenia (jednak musi wyraźnie w ofercie zaznaczyć, które usługi wypełniają warunek).
   2) w celu spełnienia warunku wymienionego w ust. 1 pkt 3 wykonawca winien wykazać dysponowanie osobami zdolnymi do realizacji zamówienia, to jest łącznie co najmniej:

a) jedną osobą:
   — posiadającą wiedzę (prawną i praktyczną) z zakresu bezpieczeństwa informacji (zwłaszcza ochrony danych osobowych),
   — posiadającą doświadczenie w przeprowadzenia audytu bezpieczeństwa informacji (zwłaszcza audytu ochrony danych osobowych) tzn. wykonała co najmniej 5 audytów wymienionych w ust. 1 lit. a,

b) jedną osobą:
   — posiadającą wiedzę (prawną i praktyczną) z zakresu informatyki (zwłaszcza ochrony teleinformatycznej, Krajowych Ram Interoperacyjności, zagrożeń teleinformatycznych),
   — posiadającą doświadczenie w przeprowadzania audytu bezpieczeństwa informacji (zwłaszcza audytu ochrony teleinformatycznej) tzn. wykonała co najmniej 5 audytów wymienionych w ust. 1 lit. b,

c) jedną osobą doświadczoną w przeprowadzaniu szkoleń z zakresu bezpieczeństwa informacji (zwłaszcza ochrony danych osobowych i bezpieczeństwa teleinformatycznego), która zrealizowała co najmniej 8 ww. szkoleń dla grupy min. 10 osób (nie szkolenie wewnętrzne wykonawcy).

Powyższe warunki może wypełniać jedna, dwie lub trzy osoby.

3. Wykonawcy niespełniający wszystkich warunków zostaną wykluczeni z postępowania. Zamawiający może wezwać do uzupełnienia lub wyjaśnienia oferty. Z postępowania zostaną również wykluczeni wykonawcy, wobec których zastosowanie ma choć jedna podstawa z art. 24 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164) (podstawa weryfikacji – oświadczenie wykonawcy).
4. Wykonawca dołączy do oferty dokumenty poświadczające spełnianie warunków określonych w ust. 2:
   1) Dokumenty poświadczające należyte wykonanie usługi np. listy referencyjne itp. (oryginał lub kopia poświadczona za zgodność z oryginałem) oraz wykaz – ust. 1 lit. a i b;
   2) wykaz – ust. 2 lit a, b i c.
5. Wykonawca dołączy do oferty szczegółowy opis swojej firmy.
6. Z postępowania zamawiający wykluczy wykonawców, których działalność będzie budziła uzasadnione wątpliwości zamawiającego.
   http://giodo.gov.pl/560/id_art/9594/j/pl/
   Oferty ich zostaną odrzucone.

VI. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Wykonawca sam opracowuje ofertę, jednak wskazane aby skorzystał ze wzoru zamawiającego. Wykonawca obowiązkowo musi dołączyć do oferty wykazy w formie tabelarycznej, w których wyraźnie uwidoczni (opisze) cechy wykazanych usług oraz załączy odpowiednie certyfikaty, które umożliwią przypisanie odpowiedniej liczby punktów w kryteriach oceny ofert.
2. Oferta powinna:
   - być opatrzony pieczątką firmową,
   - posiadać datę sporządzenia,
   - zawierać adres lub siedzibę wykonawcy, numer telefonu, numer NIP, e-maila,
   - potwierdzać warunki udziału w postępowaniu (niezbędne dokumenty),
   - być podpisana przez wykonawcę (osobę umocowaną),
   - zawierać dokument potwierdzający umocowanie osoby podpisującej ofertę,
   - umożliwiać przypisanie punktacji w każdym kryterium oceny ofert – zawierać, cenę, tabelaryczne zestawienie doświadczenia i osób (koniecznie z opisem umożliwiającym przyporządkowanie) oraz stosowne oświadczenia,
   - zawierać szczegółowy plan rzeczowo-finansowy audytu,

- zawierać projekt umowy.

3. Wykonawca wskaże w ofercie numer telefonu, pod którym będzie dostępny w godzinach pracy zamawiającego, przez cały okres trwania umowy.
4. Oferta powinny być napisane czytelnie, w języku polskim (wskazany jest wydruk komputerowy).
5. Wszelkie poprawki lub zmiany w tekście oferty muszą być parafowane własnoręcznie przez osobę podpisującą.

VII. Informacja o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń lub dokumentów. Wskazanie osób uprawnionych do porozumiewania się z wykonawcami

1. Wykonawcy mogą zwracać się do zamawiającego oraz zamawiający do wykonawców z wnioskami, pytaniami lub wyjaśnieniami pisemnie, faksem lub drogą elektroniczną. W treści pisma bądź w temacie maila prosimy wpisać znak sprawy.
2. Osobą uprawnioną przez zamawiającego do kontaktowania się z wykonawcami jest Wojciech Reutt, tel. (22) 760-70-54, e-mail: wojciech.reutt@kobylka.pl (w temacie maila prosimy wpisać znak sprawy).
3. Zamawiający zwraca się z prośbą do wykonawców o potwierdzanie odbioru pism (tą samą formą, którą pismo wpłynęło do wykonawcy). W przypadku braku potwierdzenia za datę odbioru pisma zamawiający uzna datę nadania go faksem lub za pomocą poczty elektronicznej.

VIII. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT.

1. Oferta powinna być przesłana za pośrednictwem: poczty lub kuriera na adres: Urząd Miasta Kobyłka, 05-230 Kobyłka ul. Wołomińska 1 lub też dostarczona osobiście do kancelarii Urzędu Miasta Kobyłka, do dnia **13.12.2017 r. do godz. 13^{00}, otwarcie ofert 13^{15}**
   W przypadku przesłania oferty pocztą lub przesyłką kurierską do zamawiającego, należy wziąć pod uwagę, że terminem jej dostarczenia (złożenia) zamawiającemu jest jej wpływ do miejsca oznaczonego przez zamawiającego, jako miejsce składania ofert (nie termin nadania). Zamawiający nie bierze odpowiedzialności za nieterminowe doręczanie korespondencji.

2. Ofertę wraz z załącznikami należy złożyć w zapakowanej kopercie oznaczonej:

OFERTA na
wykonanie usługi audytu bezpieczeństwa informacji
wraz z wdrożeniem RODO
w Urzędzie Miasta Kobyłka
nie otwierać przed 13.12.2017 r. godz. 13:15.

3. Oferty złożone po terminie nie będą rozpatrywane.
4. Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
5. W toku badania i oceny ofert Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert.
6. Zamawiający zastrzega sobie unieważnienie postępowania na każdym etapie bez podania przyczyny.

IX. SPOSÓB OCENY OFERT

1. Kryteria oceny ofert:

Co	cena ofertowa (Co)	30%,
D	doświadczenie (D)	20%,
Pa	ocena planu audytu (Pa)	20%
Pb	podwyższenie bezpieczeństwa (Pb)	10%
Mic	posiadanie certyfikatu Microsoft (certyfikowane uprawnienia wydane przez firmę Microsoft do weryfikowania legalności oprogramowania) (Mic)	10%,
ISO	posiadanie wdrożonego systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 (ISO)	10%,

2. Za najkorzystniejszą ofertę zostanie wybrana oferta z największą łączną liczbą punktów, która mieścić się będzie w środkach, jakie zamawiający ma zamiar przeznaczyć na realizację zamówienia.
3. Bezpośrednio przed otwarciem ofert zamawiający poda kwotę jaką ma zamiar przeznaczyć na realizację zamówienia.
4. Sposób obliczania punktacji:

Po = Co + D + Pa + Pb + Mic + ISO

Po – punktacja oferty

1) Kryterium – cena ofertowa

Wykonawca poda cenę oferty (z właściwym podatkiem od towarów i usług) za realizację przedmiotu zamówienia wyrażoną w polskiej walucie.

Punkty zostaną przyznane wykonawcy wg wzoru:

$$Co = C_n / C_b * 100 * 30\%$$

gdzie:
- Co – ilość przyznanych punktów w kryterium cena
- C_n – cena brutto najniższej oferty
- C_b – cena brutto badanej oferty

2) Kryterium – Doświadczenie

Wykonawca może wykazać tu usługę, którą wskazuje w warunku udziału w postępowaniu. W doświadczeniu w ramach kryterium oceny ofert nie ma ograniczeń czasowych.

Punktowane w kryterium będzie wyłącznie doświadczenie **własne** wykonawcy.

a) Doświadczenie w zakresie audytu ochrony danych

– w urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub oddziale wojewódzkim takiego urzędu lub sądzie lub ambasadzie lub innym centralnym organie państwowym lub jego oddziale wojewódzkim lub aktualnym urzędzie wojewódzkim lub marszałkowskim lub ich jednostkach podległych lub urzędzie administracji rządowej terenowej na poziomie województwa (administracji zespolonej lub niezespolonej) lub urzędzie miejskim

aktualnego miasta wojewódzkiego lub uczelni wyższej (mającej status uczelni akademickiej) lub państwowej jednostce badawczej lub innym podmiocie państwowym lub samorządowym zatrudniającym powyżej 800 osób (np. przedsiębiorstwo państwowe)
20 pkt. za każdy audyt,

- w urzędzie gminy/miasta o liczbie mieszkańców min. 20 tys. lub w urzędach powiatowych lub urzędach administracji rządowej terenowej na poziomie powiatu (administracji zespolonej lub niezespolonej) lub w podmiocie prywatnym zatrudniającym powyżej 200 osób
  7 pkt. za każdy audyt,
- podmioty prywatne o liczbie zatrudnionych pomiędzy 80 a 200 osób lub inne instytucje publiczne
  3 pkt. za każdy audyt,
- audyty w podmiotach innych niż ww.
  1 pkt za każdy audyt;

b) Doświadczenie w zakresie audytu bezpieczeństwa teleinformatycznego

- w urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub oddziale wojewódzkim takiego urzędu lub sądzie lub ambasadzie lub innym centralnym organie państwowym lub jego oddziale wojewódzkim lub aktualnym urzędzie wojewódzkim lub marszałkowskim lub ich jednostkach podległych lub urzędzie administracji rządowej terenowej na poziomie województwa (administracji zespolonej lub niezespolonej) lub urzędzie miejskim aktualnego miasta wojewódzkiego lub uczelni wyższej (mającej status uczelni akademickiej) lub państwowej jednostce badawczej lub innym podmiocie państwowym lub samorządowym zatrudniającym powyżej 800 osób (np. przedsiębiorstwo państwowe)
  15 pkt. za każdy audyt,
- w urzędzie gminy/miasta o liczbie mieszkańców min. 20 tys. lub w urzędach powiatowych lub urzędach administracji rządowej terenowej na poziomie powiatu (administracji zespolonej lub niezespolonej) lub w podmiocie prywatnym zatrudniającym powyżej 200 osób
  5 pkt. za każdy audyt,
- podmioty prywatne o liczbie zatrudnionych pomiędzy 80 a 200 osób lub inne instytucje publiczne
  1 pkt. za każdy audyt,
- audyty w podmiotach innych niż ww.
  0,25 pkt za każdy audyt;

c) Doświadczenie w zakresie wdrożenia systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001

- w urzędzie państwowym centralnym (to jest: ministerstwo, urząd naczelny/centralny podległy ministrowi lub premierowi) lub oddziale wojewódzkim takiego urzędu lub sądzie lub ambasadzie lub innym centralnym organie państwowym lub jego oddziale wojewódzkim lub aktualnym urzędzie wojewódzkim lub marszałkowskim lub ich jednostkach podległych lub urzędzie administracji rządowej terenowej na poziomie województwa (administracji zespolonej lub niezespolonej) lub urzędzie miejskim aktualnego miasta wojewódzkiego lub uczelni wyższej (mającej status uczelni akademickiej) lub państwowej jednostce badawczej lub innym podmiocie państwowym lub samorządowym zatrudniającym powyżej 800 osób (np. przedsiębiorstwo państwowe)
  5 pkt. za każdy audyt,
- w urzędzie gminy/miasta o liczbie mieszkańców min. 20 tys. lub w urzędach powiatowych lub urzędach administracji rządowej terenowej na poziomie powiatu (administracji zespolonej lub niezespolonej) lub w podmiocie prywatnym zatrudniającym powyżej 200 osób

1,5 pkt. za każdy audyt,
- podmioty prywatne o liczbie zatrudnionych pomiędzy 80 a 200 osób lub inne instytucje publiczne
  0,5 pkt. za każdy audyt,
- audyty w podmiotach innych niż ww.
  0,05 pkt za każdy audyt;

Wykonawca może wykazywać jedną usługę w ramach dwóch lub trzech podkryteriów.
Przykład
Za audyt danych osobowych oraz bezpieczeństwa teleinformatycznego w Zarządzie Dróg Wojewódzkich a następnie wdrożenie tam systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 wykonawca otrzyma 40 punktów. Jednak ostateczna liczba punktów będzie przydzielona wg poniższego wzoru.

A następnie punkty zostaną przeliczone na podstawie wzoru:

D = db / dn * 100 * 20%
D - liczba punktów przyznanych w kryterium doświadczenie
db - liczba punktów (suma) przyznanych na podstawie ww. lit a, b, c ofercie badanej
dn - największa liczba punktów (suma) przyznanych na podstawie ww. lit. a, b, c

3) Kryterium – ocena planu audytu

Wykonawca do oferty musi dołączyć szczegółowy plan audytu opierając się na szczegółowym opisie przedmiotu zamówienia stanowiącym załącznik do niniejszego regulaminu. Wykonawca będzie nim związany podczas realizacji przedmiotu zamówienia. Zamawiający dopuszcza zmiany w ww. planie do 30%, wówczas strony ustalą wysokość wynagrodzenia.
Plan audytu musi być spójny z szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik do niniejszego regulaminu, jednak wykonawca może zaoferować zakres szerszy.
Oceniane będą (kolejność wg wagi):
- szczegółowość planu (doszczegółowienie opisu przedmiotu zamówienia np. sposób realizacji analiz teleinformatycznych),
- podział na etapy (przejrzyste podzielenie przedmiotu zamówienia na etapy i określenie jasnych mierników zrealizowania danego etapu w tym kary za opóźnienie w ich realizacji (odzwierciedlone we wzorze umowy)),
- rozłożenie realizacji w czasie – wykonawca może skrócić czas realizacji przedmiotu zamówienia, jednak zamawiający oczekuje stopniowego równomiernego rozłożenia płatności 60% ceny oferty, zaś faktura za pozostałe 40% musi być wystawiona po wykonaniu całości przedmiotu zamówienia.
- poszerzenie przedmiotu zamówienia koniecznie ze zwięzłym uzasadnieniem,
- klauzule bezpieczeństwa i poufności (umowa).
Każdy z członków komisji oceniającej oferty przyzna od 0 do 20 punktów. Liczba przyznanych punktów ofercie będzie średnią arytmetyczną punktów przyznanych przez członków komisji.

4) Kryterium – podwyższenie bezpieczeństwa

W związku z faktem, że wybrany wykonawca będzie miał dostęp do teleinformatycznych zabezpieczeń zamawiającego oraz do sposobu ochrony danych osobowych wykonawcy, którzy zaoferują wykonanie przedmiotu zamówienia przez

osoby mające aktualne poświadczenie bezpieczeństwa o klauzuli minimum „poufne" otrzymają punkty w tym kryterium na poniższych zasadach:

a) Za oferowanie wykonania całości przedmiotu zamówienia wyłącznie przez ww. osoby wykonawca otrzyma 10 pkt.
b) Za oferowanie wykonania całości audytu teleinformatycznego oraz opracowanie nowych dokumentów związanych z ochroną danych osobowych wyłącznie przez ww. osoby wykonawca otrzyma 8 pkt.
c) Za oferowanie wykonania całości audytu teleinformatycznego wyłącznie przez ww. osoby wykonawca otrzyma 7 pkt.
d) Za oferowanie opracowania nowych dokumentów związanych z ochroną danych osobowych wyłącznie przez ww. osoby wykonawca otrzyma 3 pkt.
e) Za oferowanie nadzorowania wykonania całości przedmiotu zamówienia (min. pozytywna opinia o osobach wykonujących przedmiot zamówienia, opracowanie harmonogramu prac spójnego z planem audytu złożonym do oferty, pisemna ocena wyników audytu z propozycjami działań) wyłącznie przez ww. osoby wykonawca otrzyma 1 pkt.

Wykazane osoby nie mogą być użyczone od podmiotu trzeciego. Muszą stanowić zasób osobowy wykonawcy (umowa o prace, właściciel, członek organu zarządzającego itp.)

5) Kryterium – posiadanie certyfikatu Microsoft (certyfikowane uprawnienia wydane przez firmę Microsoft do weryfikowania legalności oprogramowania)

Sposób przyznawania punktów w kryterium posiadany certyfikat Microsoft (certyfikowane uprawnienia wydane przez firmę Microsoft do weryfikowania legalności oprogramowania).
Za posiadanie przez wykonawcę certyfikowanych uprawnień wydanych przez firmę Microsoft do weryfikowania legalności oprogramowania przyznanych zostanie 10 punktów.
Ww. certyfikat musi dotyczyć wykonawcy składającego ofertę. Nie może być udostępniony („pożyczony") od podmiotu trzeciego.
Należy złożyć stosowne oświadczenie.

Poprzez certyfikat Microsoft zamawiający rozumie każdy certyfikat wydany przez Microsoft upoważniający do weryfikacji legalności oprogramowania wystawiony na podmiot dokonujący weryfikacji (osobę fizyczną lub prawną) – mogą to być certyfikaty Volume Licensing Specialist, Large Organizations, Volume Licensing Specialist Small and Medium Organization

6) Kryterium –posiadanie wdrożonego systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 (ISO)

Sposób przyznawania punktów w kryterium wdrożony system Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001
Za wdrożony u wykonawcy system Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 przyznanych zostanie 10 pkt.
Uniemożliwia się jakiekolwiek „pożyczanie" od podmiotu trzeciego.
Należy złożyć stosowne oświadczenie.

X. UMOWA

1. Z wybrany wykonawcom zostanie podpisana umowa uwzględniająca opis przedmiotu zamówienia ustalony w trakcie postępowania (wg złożonej przez wykonawcę oferty – plan audytu i projekt umowy).
2. Minimalne kary za opóźnienie w realizacji całości przedmiotu zamówienia to 0,05% ceny oferty za każdy dzień opóźnienia do 30 dnia opóźnienia i 5% ceny oferty za każdy dzień opóźnienia od 30 dnia opóźnienia.
3. Po opublikowaniu wyniku strony przystąpią do negocjacji zapisów planu audytu i umowy (w stosunku zakres/cena). W przypadku braku porozumienia zamawiający zastrzega sobie prawo do wyboru kolejnego wykonawcy.
4. Wykonawca niezwłocznie po ww. ustaleniach, jednak przed podpisaniem umowy opracuje aktualny szczegółowy harmonogram rzeczowo-finansowy prac.
5. Zamawiający zastrzega zmiany w ww. harmonogramie po podpisaniu umowy, jednak zmiany te muszą być zaakceptowane przez obie strony.

MINIMALNY OPIS PRZEDMIOTU ZAMÓWIENIA
wraz z proponowanymi poszerzeniami (opcjonalnie)

Zakres audytu: audyt ochrony danych osobowych i bezpieczeństwa teleinformatycznego.

Ideą zamawianego audytu jest dokonanie sprawdzeń w istotnych zakresach bezpieczeństwa informacji przy pomocy racjonalnego zaangażowania pracowników i sprzętu oraz racjonalnych środków finansowych, w tym zwłaszcza wskazanie dokumentacji lub praktyki urzędu, która nie odpowiada aktualnym przepisom prawa lub ich zmianom, nieszczelności systemów teleinformatycznych lub regulacji wewnętrznych, wskazanie niezbędnych zabezpieczeń oraz opracowanie niezbędnych dokumentów.

1. Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu audytu bezpieczeństwa informacji zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych, niezbędnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016, poz. 113), wdrożenia Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO). Po przeprowadzeniu audytu wykonawca musi sporządzić dokument podsumowujący, zawierający propozycje działań dla zamawiającego z podziałem na działania niezbędne, wskazane i opcjonalne (podając uzasadnienie merytoryczne i prawne oraz szacunkowe koszty i terminy realizacji, jeżeli są określone).
2. Audyt musi obejmować dwie płaszczyzny: bezpieczeństwo teleinformatyczne i ochronę danych osobowych (w tym ochronę wizerunku).
3. Audyt musi obejmować:
   1) audyt zabezpieczeń styku sieci lokalnej i Internet w zakresie wszystkich warstw modelu ISO OSI:
      a) analiza urządzeń zapewniających Zamawiającemu dostęp do sieci Internet w tym urządzenia aktywne oraz urządzenia pasywne,
      b) analiza istniejącej na dzień przeprowadzenia audytu konfiguracji sieci lokalnej,
      c) analiza parametrów technicznych urządzeń, o których mowa w pkt 1lit. a,
      d) analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia teleinformatycznego.
   2) audyt bezpieczeństwa infrastruktury oraz serwerów:
      a) analiza budowy logicznej sieci Zamawiającego – podział na segmenty (fizyczne lub logiczne, o ile istnieją u Zamawiającego),
      b) analiza sposobu połączenia segmentów pomiędzy sobą,
      c) analiza metody komunikacji pomiędzy segmentami sieci,
      d) analiza bezpieczeństwa serwerów;
   3) audyt kopii zapasowych:
      a) analiza poprawności wykonywanych kopii zapasowych,
      b) analiza częstotliwości wykonywania kopii zapasowych,
      c) analiza bezpieczeństwa wykonywanych kopii zapasowych;
   4) audyt zabezpieczeń oraz zainstalowanego oprogramowania:
      a) analiza zainstalowanego oprogramowania znajdującego się na urządzeniach (w tym urządzeniach mobilnych np. laptopy, *tablety*, *smartfony – możliwe poszerzenie*) Zamawiającego,
      b) analiza bezpieczeństwa stacji roboczych Zamawiającego;
   5) audyt podatności systemów informatycznych Zamawiającego;
   6) inwentaryzacja sprzętu komputerowego;
   7) inwentaryzacja zbiorcza zainstalowanego oprogramowania;

8) inwentaryzacja zainstalowanego oprogramowania per komputer;
9) analiza poziomu wdrożenia dokumentacji związanej z ochroną danych osobowych w odniesieniu do stanu faktycznego systemu informatycznego Urzędu oraz ustawy o ochronie danych osobowych:
   a) analiza zgodności przetwarzania danych osobowych z wymogami ustawy o ochronie danych osobowych oraz wewnętrznymi regulacjami,
   b) zgodności dokumentacji ochrony danych osobowych z obowiązującymi przepisami prawa z uwzględnieniem RODO ;
   c) czynności powyższe wykonane zostaną po przedstawieniu przez Zamawiającego dokumentów opracowanych przez Zamawiającego dotyczących ochrony danych osobowych – tj. Polityki bezpieczeństwa informacji, Instrukcji zarządzania systemem informatycznym oraz załączników do wymienionej dokumentacji.
10) analiza poziomu wdrożenia rozporządzenia 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 *oraz zaleceń konfiguracyjnych CERT.GOV.PL (https://www.cert.gov.pl/cer/zalecenia-konfiguracyj) – opcjonalnie*;
11) Badanie - ankieta z użytkownikami mającej na celu weryfikację wiedzy oraz świadomości w zakresie bezpieczeństwa informatycznego oraz ochrony danych osobowych – opcjonalnie;
12) audyt wykorzystywania sprzętu komputerowego.
Analiza wykorzystania sprzętu komputerowego Zamawiającego przez użytkowników w okresie minimum 14 dni roboczych w zakresie przeglądanych stron www, czasu korzystania przez z poszczególnych aplikacji bądź pakietów aplikacji - opcjonalnie

4. Audyt bezpieczeństwa informacji we wszystkich obszarach funkcjonowania organizacji.
   1) audyt organizacyjny
      a) regulacje w obszarze zarządzania bezpieczeństwem informacji,
      b) odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji,
      c) dokumentacja w tym z zakresu ochrony danych osobowych,
      d) Przeprowadzenie wywiadów z wybranymi pracownikami;
   2) audyt fizyczny i środowiskowy:
      a) weryfikacja granic obszaru bezpiecznego,
      b) weryfikacja zabezpieczeń wejścia/wyjścia,
      c) weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
      d) weryfikacja bezpieczeństwa okablowania strukturalnego;
      e) weryfikacja systemów chłodzenia,
      f) weryfikacja systemów alarmowych;
   3) audyt teleinformatyczny
      a) weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,
      b) weryfikacja ochrony przed oprogramowaniem szkodliwym,
      c) weryfikacja procedur zarządzania kopiami zapasowymi,
      d) weryfikacja procedur związanych z rejestracją błędów,
      e) weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
      f) weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
      g) weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania),
      h) analiza i ocena mechanizmów zarządzania aktualizacjami;
5. Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej

1) testy styku sieci lokalnej z Internetem przeprowadzane ze stacji roboczej podłączonej do sieci Internet:
   a) analiza topologii brzegu sieci,
   b) weryfikacja mechanizmów ochronnych,
   c) próba wykrycia usług sieciowych udostępnianych do Internetu,
   d) detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet,
   e) analiza podatności na zagrożenia dostępnych urządzeń oraz usług wystawionych do sieci Internet,
   f) przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią Internet;
2) testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji
   a) analiza topologii sieci LAN,
   b) weryfikacja mechanizmów ochronnych w sieci;
   c) analiza komunikacji sieciowej,
   d) skanowanie portów TCP/UDP próba wykrycia usług sieciowych,
   e) skanowanie hostów aktywnych w sieci,
   f) eksploitacja dostępnych urządzeń oraz usług w sieci LAN,
   g) przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN;
3) audyt socjotechniczny czynnika ludzkiego
   a) próby uzyskania poufnych informacji od użytkowników – opcjonalnie,
   b) próby umieszczenia szkodliwego oprogramowania na stacjach roboczych,
   c) próby uzyskania dostępu do danych poufnych u użytkowników– opcjonalnie,
   d) sprawdzenie sposobu przechowywania haseł przez użytkowników.
   e) weryfikacja ochrony powierzonego sprzętu i dokumentacji;
4) inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji, *połączona z weryfikacją legalnością użytkowanego oprogramowania – opcjonalnie*.

6. Audyt bezpieczeństwa informacji obejmujący (ochrona danych osobowych):
   1) Dokumenty do analizy:
      a) Politykę Bezpieczeństwa, Instrukcję Zarządzania Systemem Informatycznym oraz wymagane procedury i instrukcje,
      b) dokumenty ABI'ego,
      c) dokumenty kontroli zarządczej – opcjonalnie,
      d) zakres ubezpieczenia – opcjonalnie,
      e) dokumenty systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001:2009 - opcjonalnie,
      f) Regulamin Organizacyjny UMK + *opcjonalnie inne niezbędne dokumenty*,
      g) zakresy obowiązków osobowych i wydziałów,
      h) sposób nadzorowania jednostek w zakresie ochrony danych osobowych i bezpieczeństwa teleinformatycznego pod kątem wypełniania wymogów prawa przez Urząd,
      i) ocena prawna np. sposobu publikacji i treści uchwał zawierających dane osobowe, transmisji z obrad Rady Miasta
      j) obieg dokumentów – zakres opcjonalny, jednak pożądany przez zamawiającego,
      k) ochrona tajemnicy przedsiębiorstwa – zakres opcjonalny,
      l) umowy powierzenia danych osobowych (opracowanie nowych klauzul),
      m) umowy z firmą "ochroniarską" – zakres opcjonalny, jednak pożądany przez zamawiającego,
      n) umowy z osobami sprzątającymi urząd – zakres opcjonalny
      o) ochrona wizerunku w urzędzie (posiadanie wymaganych oświadczeń) – zakres opcjonalny, jednak pożądany przez zamawiającego,

p) ochrona danych osobowych w dokumentacji osobowej (HR) pracowników (w tym Międzyzakładowy Fundusz Świadczeń Socjalnych, kasa zapomogowopożyczkowa, ubezpieczenia grupowe na życie pracowników);

2) Stan faktyczny
   a) przygotowanie zestawienia systemów informatycznych, za pomocą których przetwarzane są dane osobowe w Urzędzie Miasta Kobyłka oraz niezbędna ocena tych systemów pod kątem spełniania przez nie wymogów prawa oraz umów,
   b) sprzęt IT i oprogramowanie (w tym zwłaszcza: Komputery, serwery, telefony komórkowe)
   c) łącza internetowe (w tym bezpieczeństwo fizyczne okablowania),
   d) praktyka pracowników
      – ochrona danych osobowych (wykonawca dokona czynności tak jak w sprawdzeniu z ustawy o ochronie danych osobowych),
      – bezpieczeństwo teleinformatyczne;
3) Opracowanie zbiorów danych
   a) ocena kompletności aktualnych zbiorów danych,
   b) wskazanie ew. niezgłoszonych zbiorów wraz z ich zarejestrowaniem,
   c) przeprowadzenie sprawdzeń (o których mowa w ustawie o ochronie danych osobowych) wszystkich zbiorów danych.

7. Przygotowanie/opracowanie dokumentów:
   1) Nowe dokumenty dotyczące ochrony danych osobowych – wymagane na podstawie RODO;
   2) nowe dokumenty ABI'ego (formularze) *i kontroli zarządczej – zakres opcjonalny;*
   3) Polityka zakupowa (w oparciu o PZP, jeżeli zachodzi konieczność stosowania) uwzględniająca szacowane koszty – zakres opcjonalny, jednak pożądany przez zamawiającego:
      a) sprzętu IT
      b) oprogramowania,
      c) *innego wyposażenia urzędu – w tym pomoc w opisie przedmiotu zamówienia (ocena przygotowanych opisów).*
   4) Propozycje zmiany zakresu ubezpieczenia – zakres opcjonalny,
   5) ocena propozycji ubezpieczeń ryzyk cybernetycznych;
   6) Jeżeli zajdzie taka potrzeba uzupełnienie informacji i wdrożenie zmian odnośnie
      a) kontroli zarządczej – zakres opcjonalny,
      b) systemu zarządzenia jakością zgodnego z normą PN-EN ISO 9001:2009 – zakres opcjonalny,
      c) zakresu obowiązków i Regulaminu Org. UMK,
      d) w innych dokumentach – zakres opcjonalny;
   5) propozycje zmian w nadzorowaniu jednostek (oraz podmiotów, którym Miasto Kobyłka przekazuje dane osobowe) w zakresie ochrony danych osobowych i bezpieczeństwa teleinformatycznego (wypełnienie wymogów prawa przez Urząd);
   6) opracowanie szczegółowej analizy ryzyka i oszacowanie ryzyk w obrębie badanych zagadnień (*w oparciu o normę PN-ISO/IEC 27005:2014– zakres opcjonalny*):
      a) inwentaryzacja aktywów podlegających szacowaniu ryzyka,
      b) określenie zagrożeń dla wyznaczonych aktywów,
      c) określenie podatności dla wyznaczonych aktywów,
      d) określenie prawdopodobieństw dla wyznaczonych aktywów,
      e) oszacowanie ryzyka pod kątem skutków naruszenia bezpieczeństwa informacji;
   7) wykonanie i przekazanie Raportów z Audytu z omówieniem;
   8) jeżeli zajdzie taka potrzeba odniesienie się we wszystkich ocenach do Krajowych Ram Interoperacyjności;

8. Szczegółowe zapoznanie ADO, ABIego i ASIego z wynikami audytu oraz szkolenie ww. z nowych procedur i nowych wymogów prawa (zwłaszcza RODO, KRI).
9. Szkolenie dla pracowników (i ew. osób z jednostek organizacyjnych Miasta Kobyłka) obejmujące problematykę:
   1) ochronę danych osobowych i ochronę wizerunku oraz bezpieczeństwa teleinformatycznego w tym:
      a) omówienie zasad bezpieczeństwa informacji,
      b) zagrożenia bezpieczeństwa informacji,
      c) skutki naruszenia zasad bezpieczeństwa informacji,
      d) stosowanie środków zapewniających bezpieczeństwo informacji,
      e) zasady zgłaszania i reagowania na incydenty;
   2) nowe rozwiązania (min. omówienie nowej Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym).

   Osoba szkoląca musi podczas szkolenia przewidywać możliwość zadawania pytań przez uczestników z zakresu przedmiotu zamówienia, a zakres wiedzy osoby szkolącej musi umożliwić jej odpowiedzenie.

   Szkolenie realizowane przez osobę doświadczoną w szkoleniach z zakresu bezpieczeństwa informacji (min. 5 szkoleń w ciągu 12 następujących po sobie miesięcy). W szkoleniu nie może brać udział więcej niż ok. 20-25 osób (uwzględniając liczbę pracowników potrzeba ok. 5-7 szkoleń).

   Oczekiwany podział grup pracowników:

   - Zarząd Miasta Kobyłka (Burmistrz Miasta, zastępcy burmistrza, Skarbnik Miasta, Sekretarz Miasta),
   - dyrektorzy i pracownicy jednostek,
   - *radni Miasta Kobyłka – zakres opcjonalny,*
   - kierownicy wydziałów i stanowiska samodzielne (ok. 15 osób),
   - *pracownicy tura 1,*
   - *pracownicy tura 2,*
   - *pracownicy tura 3 – zakres opcjonalny.*
10. Wdrożenie niezbędnych dokumentów i procedur wymaganych w RODO w jednostkach podległych (Biblioteka Publiczna, Miejski Ośrodek Kultury, Ośrodek Sportu i Rekreacji) w tym rejestracja zbiorów i pierwszy ich audyt.
11. *Zapewnienie rocznej opieki doradczej po zakończeniu audytu – zakres opcjonalny.*
12. Wykonawca wskaże jedną osobę odpowiedzialną za koordynację i postęp prac.

Dane zamawiającego

Urząd Miasta Kobyłka

- zatrudnia ok. 90 osób,
- ok. 30 adresów IP publicznych i 120 adresów IP prywatnych,
- Komputerów (stacji roboczych) ok. 100 szt. (w tym ok. 20 szt. laptopów) – wszystkie system operacyjny - objęte podstawowym zakresem audytu,
- Serwerów ok. 3 szt. (w obecnej chwili 1 szt. serwer Linux, ale zamawiający planuje odejść tego systemu operacyjnego, pozostałe serwery mają system operacyjny Windows) - objęte podstawowym zakresem audytu,
- Tabletów ok. 30 szt. (ok. 29 szt. na systemie operacyjnym Android i 1 szt. na iOS) *nie objęte podstawowym zakresem audytu (możliwość poszerzenia w ramach kryteriów)*,
- Smartfonów ok. 24 szt. (Android ok. 20 szt., Windows Phone ok. 2 szt., iOS ok. 2 szt.) *nie objęte podstawowym zakresem audytu (możliwość poszerzenia w ramach kryteriów)*,

Miejski Ośrodek Kultury

- zatrudnienie ok. 8 osób,
- 1 adres IP publiczny i ok. 10 adresów IP prywatnych, - komputerów (stacji roboczych) ok. 6 Telecentrum, 7 MOK szt. (w tym ok. 5 szt. laptopów) – wszystkie system operacyjny Windows,
- smartfonów ok. 3 szt. (Android ok. 3 szt.)

Ośrodek Sportu i Rekreacji

- zatrudnienie ok. 9 osób,
- ok. 1 adresów IP publicznych i 0 adresów IP prywatnych,
- komputerów (stacji roboczych) ok. 3 szt. (w tym ok. 2 szt. laptopów) – wszystkie system operacyjny Windows,

Miejska Biblioteka Publiczna

- zatrudnienie ok. 10 osób,
- 1 adres IP publiczny dla wielu jednostek i ok 10 adresów IP prywatnych,
- komputerów (stacji roboczych) ok. 10 szt. (w tym ok. 0 szt. laptopów) – wszystkie system operacyjny Windows,