PREZYDENT MIASTA OTWOCKA
ul. Armii Krajowej 5, 05-400 Otwock
tel.: +48 (22) 779 20 01 (do 06); fax: +48 (22) 779 42 25
www.otwock.pl e-mail: umotwock@otwock.pl

Otwock, dnia 20.10 roku. 2021

ZAPYTANIE OFERTOWE

Urząd Miasta Otwocka zaprasza do składania ofert na wykonanie zamówienia pn:

„Przeprowadzenie audytu bezpieczeństwa systemu informatycznego oraz bezpieczeństwa informacji w Urzędzie Miasta Otwocka."

I. Zaproszenie

Urząd Miasta Otwocka zaprasza do złożenia oferty cenowej na usługę przeprowadzenia audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audytu bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji w Urzędzie Miasta Otwocka. Audyt ma na celu ustalenie aktualnego stanu całego systemu informatycznego Zamawiającego. Przedmiot zamówienia obejmuje również 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 metodą, która gwarantuje rzetelność oceny bieżącego stanu bezpieczeństwa systemów informatycznych, zgodnie z poniższymi założeniami:

II. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji 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 r. 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 zapytanie Wykonawcy w

trakcie realizacji audytowych i jest bezterminowe.

III. Obszary kontroli:

1. Przetwarzanie i ochrona danych osobowych.
2. Bezpieczeństwo systemów informatycznych.
3. Zasoby informatyczne.

IV. Szczegółowy zakres przetwarzania i ochrony danych osobowych:

1. Sprawdzenie ustalonych zasad bezpieczeństwa pod względem zgodności z obowiązującymi aktami prawnymi.
2. Analiza posiadanej przez Zamawiającego dokumentacji związanej z przetwarzaniem danych osobowych.
3. Weryfikacja realizacji przez Inspektora Ochrony Danych (IOD), wymaganych czynności.
4. Weryfikacja czynności związanych z upoważnieniem do przetwarzania danych osobowych.
5. Ocena adekwatności struktury organizacyjnej pionów IT w odniesieniu do bezpieczeństwa systemów informatycznych.
6. Weryfikacja identyfikatorów użytkowych z rejestrem osób upoważnionych do przetwarzania danych osobowych.
7. Weryfikacja wykonanych aktualizacji regulacji wewnętrznych.
8. Sprawdzenie dostępności i zapewnienia niezbędnych szkoleń dla pracowników.
9. Weryfikacja zgodności nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w systemach informatycznych z ustaloną polityką.
10. Ocena monitorowania incydentów i problemów w zakresie bezpieczeństwa IT.
11. Adekwatność i aktualność polityk, procedur i instrukcji w zakresie kopii zapasowych.
12. Weryfikacja i ocena procedur w zakresie zapewnienia ciągłości działania systemów informatycznych.
13. Weryfikacja sposobu nadawania uprawnień do przetwarzania danych osobowych oraz do prac w systemach informatycznych.

V. Szczegółowy zakres bezpieczeństwa systemów informatycznych:

1. Weryfikacja częstotliwości i sposobu zmiany haseł przez użytkowników.
2. Weryfikacja zgodności stosowanych haseł z obowiązującymi przepisami.
3. Weryfikacja podatności systemu informatycznego na ingerencje ze strony osób trzecich:

a. przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz mających na celu zidentyfikowanie podatności na włamanie,

b. przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz sieci Zamawiającego,

c. próba wykrycia usług sieciowych udostępnianych do Internetu,

d. detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet,

e. eksploatacja dostępnych urządzeń oraz usług wystawionych do sieci Internet,

f. eksploatacja dostępnych urządzeń oraz usług w sieci wewnętrznej,

g. skanowanie portów TCP/UDP i próba wykrycia usług sieciowych,

h. skanowanie hostów aktywnych w sieci,

i. weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,

j. weryfikacja ochrony przed szkodliwym oprogramowaniem,

k. weryfikacja procedur związanych z rejestracją błędów,

l. weryfikacja procedur do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania.

4. Sprawdzenie podatności serwisów internetowych.

5. Weryfikacja podatności hostów na możliwości uzyskania nieautoryzowanego dostępu do zasobów plikowych.

6. Weryfikacja podatności hostów na możliwości uzyskania nieautoryzowanego zdalnego (przez WWW) dostępu do paneli administracyjnych.

7. Istniejące zabezpieczenia logiczne na styku sieci lokalnej z Internetem.

8. Weryfikacja poprawności aktualizacji systemu informatycznego.

9. Weryfikacja poprawności aktualizacji zabezpieczeń antywirusowych.

10. Weryfikacja zabezpieczeń fizycznych, zasilania awaryjnego (testy, szkolenia użytkowników).

11. Sprawdzenie wyposażenia i zabezpieczenia pomieszczeń serwerowni.

12. Weryfikacja wykonania i sprawdzenia kopii zapasowych (częstotliwość wykonywania, miejsce przechowywania, osoby odpowiedzialne).

13. Postępowanie w przypadku incydentu naruszenia bezpieczeństwa informacji.

14. Postępowanie w zakresie utrzymania dokumentacji zabezpieczę i systemów informatycznych.

15. Dokumentowanie konfiguracji systemów służących przetwarzaniu danych osobowych.

16. Konfiguracja urządzeń sieciowych.

17. Określenie istotnych danych i istotnych zasobów informatycznych.

18. Monitorowanie bezpieczeństwa, wydajności i awarii infrastruktury informatycznej.

VI. Szczegółowy zakres zasobów informatycznych:

1.Ewidencja oprogramowania dopuszczonego do użytkowania.

2.Ewidencja przeprowadzonych kontroli w zakresie legalności oprogramowania instalowanego na stacjach roboczych.

3.Zasady zarządzania oprogramowaniem.

4.Zapewnienie bezpieczeństwa danych przy dokonywaniu napraw sprzętu i oprogramowania.

5.Wyznaczenie osób uprawnionych do dokonywania napraw sprzętu i oprogramowania.

6.Istnienie i adekwatność procedur obsługi komputerów oraz pracy sieci.

7.Inwentaryzacja sprzętu działającego w infrastrukturze informatycznej.

8.Inwentaryzacja usług sieciowych z opisem wzajemnych zależności tych usług.

9.Inwentaryzacja baz danych ze wskazaniem aplikacji korzystających z tych baz.

10.Inwentaryzacja używanych aplikacji ze wskazaniem administratorów tych aplikacji.

11.Nadzór nad zasobami informatycznymi w zakresie zakupów i wymiany sprzętu.

12.Zarządzanie aplikacjami (wykaz licencji i aplikacji, zasady dostępu do aplikacji, monitorowanie instalacji oprogramowania oraz osoby nadzorujące).

13.Fizyczne zabezpieczenia obszarów przetwarzania danych.

14. Zabezpieczenie i wyposażenie serwerowni.

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

VII. Wymagane rezultaty audytu

1.Wykonawca sporządzi sprawozdanie audytowe, które będzie zawierać:

a) Szczegółowy opis i ocenę stanu wszystkich obszarów podlegających audytowi.

b) Wykaz wszystkich problemów oraz wynikających z tego ryzyk wraz z oceną ryzyka wystąpienia wykrytych zagrożeń – propozycję rozwiązań technicznych, fizycznych oraz systemowych.

c) Zalecenia dotyczących sposobów, metod i środków usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyka.

d) Przygotowaną przez Wykonawcę aktualizację i uzupełnienie zestawu dokumentów Polityki Bezpieczeństwa zgodną z aktualnie obowiązującymi aktami prawnymi. Dokumenty te Wykonawca przygotuje w porozumieniu z Zamawiającym, uwzględniając specyfikę działań i organizację pracy Zamawiającego.

e) Opracowana dokumentacja ma zapewnić możliwość zaimplementowania zmian określonych w Rozporządzeniu ogólnym o ochronie danych osobowych/RODO/.

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

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

h) 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 zwielokrotnienie 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 jakiejkolwiek inne zmiany.

VIII. Warunki udziału w postępowaniu

1.Wiedza i doświadczenie:

Zamawiający uzna, że Wykonawca spełnia warunek wiedzy i doświadczenia, gdy Wykonawca w okresie ostatnich dwóch lat przed upływem składania ofert wykonał lub wykonuje co najmniej pięć usług odpowiadających swoim rodzajem usługą stanowiącym przedmiot zamówienia.

Na potwierdzenie spełnienia warunków w zakresie wiedzy i doświadczenia Wykonawca zobowiązany jest przedłożyć wykaz usług, zgodnie ze wzorem stanowiącym załącznik nr 2 do zapytania ofertowego.

2.Osoby zdolne do wykonania zamówienia:

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy wykażą, że dysponują lub będą dysponować osobą lub osobami, które będą uczestniczyć w wykonaniu zamówienia, spełniającymi następujące wymagania, przy czym muszą one posiadać przynajmniej po 1 certyfikacie z wymienionych poniżej:

a) Posiadać doświadczenie w zakresie przeprowadzenia audytów/testów odpowiadających swoim zakresem przedmiotowi niniejszego zamówienia oraz co najmniej jeden aktualny certyfikat z przedstawionych poniżej:
   - Certified Internal Auditor
   - Certified Information System Auditor
   - Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2021 r. poz. 514), w zakresie certyfikacji osób
   - Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z

przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,

- Certified Information Security Manager
- Certified in Risk and Information Systems Control
- Certified in the Governance of Enterprise IT
- Certified Information Systems Security Professional
- System Security Certified Practitioner
- Certified Relibiability Professional
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cyberseciurity Expert, lub równoważny

3. Wykonawca przedstawi kopie potwierdzone za zgodność z oryginałem certyfikatów osób/y będących, wymienione w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

IX. Informacje uzupełniające:

- liczba stacji roboczych w Urzędzie ok 170
- liczba serwerów fizycznych: 4

X. Kryterium oceny oferty:

Cena – 75%

25 % doświadczenie polegające na przeprowadzeniu więcej niż 15 działań audytowych w jednostkach budżetowych w ciągu ostatnich 24 miesięcy:

- 15 i mniej działań audytowych – 0 pkt
- 16-20 działań audytowych – 5 pkt
- 21- 30 działań audytowych – 10 pkt
- powyżej 30 działań audytowych – 25 pkt

XI. Miejsce i termin złożenia oferty cenowej:

1. Formularz oferty cenowej należy złożyć:

a) w formie papierowej osobiście lub pocztą na adres: Urząd Miasta Otwocka, ul. Armii Krajowej 5, 05-400 Otwock, z dopiskiem: ***„OFERTA CENOWA na Przeprowadzenie audytu bezpieczeństwa systemu informatycznego oraz bezpieczeństwa informacji w Urzędzie Miasta Otwocka”.*** Oferta musi wpłynąć do dnia 28.10.2021 r. do godziny 16^{00}

LUB

b) za pośrednictwem poczty elektronicznej na adres: umotwock@otwock.pl w terminie do dnia 28.10.21 r. do godz. 13^{00}, z dopiskiem w temacie: ***„OFERTA***

CENOWA na Przeprowadzenie audytu bezpieczeństwa systemu informatycznego oraz bezpieczeństwa informacji w Urzędzie Miasta Otwocka"

2. Opis sposobu przygotowania oferty cenowej:
   - ceny w ofercie mają być wyrażone cyfrowo i słownie
   - oferta ma być napisana w języku polskim, czytelną i trwałą techniką.
   - być opatrzona pieczątką firmową,
   - posiadać datę sporządzenia,
   - zawierać adres lub siedzibę oferenta, numer telefonu, e-mail, numer NIP
   - zawierać czytelny podpis wnioskodawcy
   - oferta musi zawierać wykaz działań audytowych w jednostkach budżetowych w ciągu ostatnich 24 miesięcy
3. Oferta cenowa otrzymana przez Zamawiającego po terminie podanym powyżej zostanie zwrócona Dostawcy nie otwarta.
4. Dostawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę cenową przed terminem upływu jej składania.

XII. Miejsce i termin otwarcia ofert.

Otwarcie złożonych ofert cenowych nastąpi w dniu 29.10.2021 o godzinie 11⁰⁰ w siedzibie Zamawiającego przy ul. Armii Krajowej 5 w Otwocku, budynek (pok. Nr 5

XIII. Wymagany termin realizacji zamówienia.

Do 21 dni od dnia podpisania umowy.

XIV. Inne istotne warunki zamówienia:

1.Umowa zostanie podpisana z Wykonawcą którego oferta została uznana za najkorzystniejszą.

2.Jeżeli Wykonawca, którego oferta została wybrana uchyli się od zawarcia umowy, Zamawiający wybierze kolejną ofertę najkorzystniejszą spośród złożonych ofert, bez przeprowadzenia ich ponownej oceny.

3.Zamawiający powiadomi o wyniku postępowania, zamieszczając stosowne ogłoszenie w Biuletynie Informacji Publicznej Urzędu Miasta Otwocka, zaś Oferent, którego oferta zostanie wybrana zostanie powiadomiony telefoniczne.

XV. Osobami uprawnionymi do kontaktów z wykonawcami są:

Pan Łukasz Samorański Naczelnik Wydziału Informatyki e-mail: lsamoranski@otwock.pl

XVI. Zamawiający ma prawo wezwania Wykonawcy do uzupełnienia dokumentów oraz wyjaśnień

XVII. Zamawiający ma prawo wykluczyć Wykonawcę i/lub odrzucić jego ofertę jeżeli Wykonawca/oferta nie spełnia wymagań określonych przez Zamawiającego

XVIII. Zamawiający ma prawo do przeprowadzenia omyłek rachunkowych, pisarskich lub innych nie powodując istotnych zmian w treści oferty.

XIX. Zamawiający zastrzega sobie prawo do unieważnienia przedmiotowego postępowania bez podania przyczyny.

z up. Prezydenta Miasta Otwocka
Piotr Bartoszewski
Sekretarz Miasta

Samowiski tuhaz

ADWOKAT
Jarosław Dąbrowski