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 ..05.11.2019 r.

ZAPYTANIE OFERTOWE

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

„Przeprowadzenie audytu informatycznego wraz z analizą ryzyka 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 audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji wraz z analizą ryzyka w Urzędzie Miasta Otwocka. 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 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 2016, poz. 113).

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.

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 Danych Osobowych (IDO), wymaganych czynności.
4. Weryfikacja czynności związanych z upoważnianiem do przetwarzania danych osobowych.
5. Ocena adekwatności struktury organizacyjnej pionów IT w odniesieniu do bezpieczeństwa systemów informatycznych.
6. Weryfikacja identyfikatorów użytkowników z rejestrem osób upoważnionych do przetwarzania danych osobowych.
7. Weryfikacja wykonywania aktualizacji regulacji wewnętrznych.
8. Sprawdzenie czytelności podziału zadań i obowiązków, wyznaczenie i podporządkowanie IDO i Administratora Sieci Informatycznej (ASI) oraz powierzenie zadań z zakresu bezpieczeństwa.
9. Sprawdzenie dostępności i zapewnienia niezbędnych szkoleń dla pracowników.
10. Weryfikacja zgodności nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w systemach informatycznych z ustaloną polityką.
11. Ocena monitorowania incydentów i problemów w zakresie bezpieczeństwa IT.
12. Adekwatność i aktualność polityk, procedur i instrukcji w zakresie kopii zapasowych.
13. Weryfikacja i ocena procedur w zakresie zapewnienia ciągłości działania systemów informatycznych.
14. Weryfikacja sposobu nadawania uprawnień do przetwarzania danych osobowych oraz do pracy 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 dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania.
4. Sprawdzenie podatności serwisów internetowych.
5. Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych.
6. Weryfikacja podatności hostów na możliwość 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 wykonywania i sprawdzania kopii zapasowych (częstotliwość wykonywania, miejsce przechowywania, osoby odpowiedzialne).
13. Postępowanie w przypadku incydentu naruszenia bezpieczeństwa informacji.

14. Postępowanie w zakresie utrzymania dokumentacji zabezpieczeń 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 prowadzonych 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 w 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 rekomendacje 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:

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 ryzyka. Lista poprawek do zainstalowania oraz szczegółowy opis zalecanych zmian konfiguracji.

6) 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 działania i organizację pracy Zamawiającego.

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

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

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

a) odtwarzanie,
b) 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,
c) przekazywanie,
d) przechowywanie,
e) wyświetlanie,
f) wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji,
g) tłumaczenie,
h) przystosowywanie,
i) zmiany układu lub jakiekolwiek 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 trzech lat przed upływem terminu składania ofert (a jeżeli okres

prowadzenia działalności jest krótszy - w tym okresie) wykonał lub wykonuje co najmniej dziesięć usług odpowiadających 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 należycie.

2. Osoby zdolne do wykonania zamówienia:

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy wykażą, że dysponują zespołem, składającym się z co najmniej dwóch osób, które będą uczestniczyć w wykonaniu zamówienia, w tym Audytora Wiodącego, spełniającego następujące wymagania:

   Ekspert ds. audytu IT i bezpieczeństwa - posiadający następujące kwalifikacje i doświadczenie zawodowe:

a) posiada co najmniej 3-letnie doświadczenie w zakresie przeprowadzania audytów odpowiadających swoim zakresem przedmiotowi niniejszego zamówienia;
b) posiada uprawnienia audytora wewnętrznego w jednostkach sektora publicznego;
c) posiada aktualny certyfikat Audytora Wiodącego norm ISO 27001, ISO 22301.

2. Drugi członek zespołu audytującego musi posiadać aktualny certyfikat: Audytor wewnętrzny ISO 27001.

3. **Wykonawca przedstawi kopie potwierdzone za zgodność z oryginałem certyfikatów osób/y będących Ekspertami ds. audytu IT i bezpieczeństwa, 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: 170
- liczba serwerów fizycznych: 3
- liczba użytkowanych systemów IT: 20
- liczba pracowników: 160

X. Kryterium oceny ofert:

Cena – 100%

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 informatycznego wraz z analizą ryzyka w Urzędzie Miasta Otwocka.** Oferta musi wpłynąć do dnia 12.11.2019 r. o godziny 16^{00}

LUB

   b. za pośrednictwem poczty elektronicznej na adres: **mmnowak@otwock.pl** w terminie do dnia 12.11.2019 r. do godz. 13^{00}, z dopiskiem w temacie: ***„OFERTA CENOWA na*** **Przeprowadzenie audytu informatycznego wraz z analizą ryzyka w Urzędzie Miasta Otwocka.**

2. Opis sposobu przygotowania oferty cenowej:
   a) Ceny i termin wykonania zamówienia w ofercie mają być wyrażone cyfrowo i słownie.
   b) Oferta ma być napisana w języku polskim, czytelną i trwałą techniką.
3. Oferta powinna:
   a) być opatrzona pieczątką firmową,
   b) posiadać datę sporządzenia,
   c) zawierać adres lub siedzibę oferenta, numer telefonu, e-mail, numer NIP,
   d) zawierać czytelny podpis Wykonawcy.
4. Oferta powinna zawierać cenę jednostkową brutto,
5. Oferta cenowa otrzymana przez Zamawiającego po terminie podanym powyżej zostanie zwrócona Dostawcy nie otwarta, lub zostanie e-mailem odesłana informacja o przekroczonym terminie wpłynięcia oferty.
6. Dostawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę cenową przed terminem upływu jej składania.

XII. Wymagany termin realizacji zamówienia.

Do 21 dni od dnia podpisania umowy.

XIII. Warunki udziału w postepowaniu.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu tj.:
   1) Wykonawca nie zalega z opłacaniem podatków, lub uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu oraz nie zalega z opłacaniem składek na ubezpieczenia zdrowotne i społeczne, lub uzyskał przewidziane prawem zwolnienie,

odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.

Na potwierdzenie ww. wykonawca złoży oświadczenie – załącznik nr 4 (w przypadku wspólnego ubiegania się o udzielenie niniejszego zamówienia przez dwóch lub więcej Wykonawców w ofercie muszą być złożone oświadczenia dla każdego z nich).

XIV. Inne istotne warunki zamówienia:

1. Umowa zostanie podpisana z Wykonawcą oferującym najkorzystniejszą cenę.
2. Jeżeli Wykonawca, którego oferta została wybrana uchyli się od zawarcia umowy, Zamawiający wybierze kolejną ofertę najkorzystniejszą spośród złożonych ofert, bez przeprowadzania 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 telefonicznie.

XV. Osobami uprawnionymi do kontaktów z wykonawcami są:

- Pani Małgorzata Nowak – Zastępca Naczelnika Wydziału Organizacyjnego
  tel: 22 779 20 01 w. 301 lub 168;
  e-mail: mmnowak@otwock.pl z tytułem: ***PYTANIE DO OFERTY Przeprowadzenie audytu informatycznego wraz z analizą ryzyka w Urzędzie Miasta Otwocka;***
- Pan Piotr Bąk– Naczelnik Wydziału Informatyki
  Tel: 22 779 20 01 w. 222
  e-mail: pbak@otwock.pl z tytułem: ***PYTANIE DO OFERTY Przeprowadzenie audytu informatycznego wraz z analizą ryzyka w Urzędzie Miasta Otwocka.***

X. Zamawiający ma prawo wezwania Wykonawcy do uzupełnienia dokumentów (nie dotyczy formularza oferty) oraz wyjaśnień.

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

XII. Zamawiający ma prawo do poprawienia omyłek rachunkowych, pisarskich lub innych nie powodujących istotnych zmian w treści oferty.

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

W załączeniu:
Załącznik nr 1 – oferta
Załącznik nr 2 – wykaz usług
Załącznik nr 3 – wykaz osób
Załącznik nr 4 – oświadczenie
Załącznik nr 5 – draft umowy

Naczelnik
Wydziału Informatyki
Piotr Bąk

Z up. Prezydenta Miasta Otwocka
Piotr Bartoszewski
Sekretarz Miasta

ADWOKAT
Jarosław Dąbrowski

Załącznik nr 1 do Zapytania ofertowego.

_____
pieczęć firmowa Wykonawcy
Nazwa / Imię i nazwisko Wykonawcy:
_____
_____
Adres: _____
Nr tel.: _____ Nr faksu: _____
Adres e-mail: _____

OFERTA

z dnia _____

dotycząca zadania pt.: *Przeprowadzenie audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji wraz z analizą ryzyka w Urzędzie Miasta Otwocka"*

1. Niniejszym oferujemy wykonanie usługi, zgodnie z warunkami zawartymi w zapytaniu i opracowaniami technicznymi załączonymi do niniejszego zapytania ofertowego za kwotę:

   - netto: _____ PLN,
   - VAT – ___%, wartość _____ PLN,
   - brutto: _____ PLN.

   słownie brutto: _____

2. Oświadczenie Wykonawcy:

   2.1 Oświadczam, że spełniam wszystkie wymagania zawarte w Zapytaniu ofertowym.

   2.2 Oświadczam, że uzyskałem od Zamawiającego wszelkie informacje niezbędne do rzetelnego sporządzenia niniejszej oferty.

   2.3 Oświadczam, że uznaję się za związanego treścią złożonej oferty, przez okres 30 dni od daty jej złożenia.

   2.4 Oświadczam, że znane mi są zasady wyboru Wykonawcy i nie wnoszę do nich zastrzeżeń.

_____ _____

(miejscowość, data) *(podpis)*

Załącznik nr 2 do Zapytania ofertowego.

WYKAZ USŁUG

Nawiązując do zapytania ofertowego na „Przeprowadzenie audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji wraz z analizą ryzyka w Urzędzie Miasta Otwocka", niniejszym przekazuję wykaz usług wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane, oraz załączeniem dowodów określających czy te usługi zostały wykonane lub są wykonywane należycie.

Nazwa i adres Wykonawcy .....

.....

Doświadczenie w zakresie wykonanych lub wykonywanych usług:

Usługi dotyczące warunku udziału w postępowaniu (nazwa usługi)	**Przedmiot usługi**	**Odbiorca usługi**	**Wartość usługi**	**Termin wykonania usługi**
Usługa 1				
Usługa 2				
.....				

_____ dnia _____ 2019 rok

(pieczęć i podpis Wykonawcy)

W załączeniu:

— dokumenty potwierdzające doświadczenie Wykładowcy tj. kopie referencji lub innych dokumentów poświadczone za zgodność z oryginałem przez Wykonawcę

Załącznik nr 3 do Zapytania ofertowego.

WYKAZ OSÓB

które będą uczestniczyć w wykonywaniu zamówienia

Nawiązując do zapytania ofertowego na „Przeprowadzenie audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji wraz z analizą ryzyka w Urzędzie Miasta Otwocka", niniejszym przekazuję wykaz osób, wchodzących w skład zespołu, który będzie wykonywać zamówienie wraz z informacjami na temat ich wykształcenia, doświadczenia i kwalifikacji niezbędnych do wykonania zamówienia, a także informacją o podstawie do dysponowania tymi osobami

Nazwa i adres Wykonawcy

.....

.....

.....

Lp.	**Imię i nazwisko**	**Wymagane doświadczenie**	**Wymagane kwalifikacje (wskazanie posiadanych certyfikatów)**	**Podstawa do dysponowania**
1.				
2.				

_____ dnia _____ 2019 rok

(pieczęć i podpis Wykonawcy)

Załącznik Nr 4 do Zapytania ofertowego

pieczęć firmowa Wykonawcy

Nazwa / Imię i nazwisko Wykonawcy:

_____

_____

Adres: _____

Nr tel.: _____ Nr faksu: _____

Adres e-mail: _____

„Przeprowadzenie audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji wraz z analizą ryzyka w Urzędzie Miasta Otwocka"

OŚWIADCZAM, że:

nie podlegam wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie przesłanek o których mowa w ust. XII pkt. 1. zapytania ofertowego.

_____ _____

(miejscowość, data) *(podpis)*

UMOWA Nr WOR.1330. .2019

W dniu ..... **2019 r.** pomiędzy Miastem Otwock, ul. Armii Krajowej 5, 05-400 Otwock, reprezentowanym przez:

.....,

zwanego w dalszej części umowy **„Zleceniodawcą",**

a

.....

..... zwanego w dalszej części umowy **„Zleceniobiorcą"**

zwani w dalszej części łącznie „**Stronami**", a każdy oddzielnie „**Stroną**".

na podstawie art. 4 pkt. 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2019 r. poz. 1843) została zawarta umowa o następującej treści:

§ 1

Przedmiot umowy

1. Przedmiotem niniejszej umowy jest wykonanie usługi polegającej na Przeprowadzeniu audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji wraz z analizą ryzyka w Urzędzie Miasta Otwocka, w tym sporządzeniu raportu z wykonanych czynności (dalej: **Usługi**) w terminie i na warunkach określonych w Umowie.
2. Zakres czynności do przeprowadzenia których zobowiązuje się Zleceniobiorca w ramach niniejszej umowy określono w § 2.

§ 2

Zakres czynności

I. Obszary kontroli:

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

II. Szczegółowy zakres przetwarzania i ochrony danych osobowych:

1. Sprawdzenie ustalonych zasad bezpieczeństwa pod względem zgodności z obowiązującymi aktami prawnymi.

2. Analiza posiadanej przez Zleceniodawcę dokumentacji związanej z przetwarzaniem danych osobowych.

3. Weryfikacja realizacji, przez Inspektora Danych Osobowych (IDO), wymaganych czynności.

4. Weryfikacja czynności związanych z upoważnianiem do przetwarzania danych osobowych.

5. Weryfikacja kwalifikacji, odbytych szkoleń, zakresu uprawnień i odpowiedzialności pracowników pionów IT.

6. Ocena adekwatności struktury organizacyjnej pionów IT w odniesieniu do bezpieczeństwa systemów informatycznych.

7. Weryfikacja identyfikatorów użytkowników z rejestrem osób upoważnionych do przetwarzania danych osobowych.

8. Weryfikacja wykonywania aktualizacji regulacji wewnętrznych.

9. Sprawdzenie czytelności podziału zadań i obowiązków, wyznaczenie i podporządkowanie IDO i Administratora Sieci Informatycznej (ASI) oraz powierzenie zadań z zakresu bezpieczeństwa.

10. Sprawdzenie dostępności i zapewnienia niezbędnych szkoleń dla pracowników.

11. Weryfikacja zgodności nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w systemach informatycznych z ustaloną polityką.

12. Ocena monitorowania incydentów i problemów w zakresie bezpieczeństwa IT.

13. Adekwatność i aktualność polityk, procedur i instrukcji w zakresie kopii zapasowych.

14.Weryfikacja i ocena procedur w zakresie zapewnienia ciągłości działania systemów informatycznych.

15. Weryfikacja sposobu nadawania uprawnień do przetwarzania danych osobowych oraz do pracy w systemach informatycznych.

III. 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 Zleceniodawcy,

   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 dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania.

4. Sprawdzenie podatności serwisów internetowych.

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

6. Weryfikacja podatności hostów na możliwość 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 wykonywania i sprawdzania kopii zapasowych (częstotliwość wykonywania, miejsce przechowywania, osoby odpowiedzialne).

13. Postępowanie w przypadku incydentu naruszenia bezpieczeństwa informacji.

14. Postępowanie w zakresie utrzymania dokumentacji zabezpieczeń 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.

IV. Szczegółowy zakres zasobów informatycznych:

1. Ewidencja oprogramowania dopuszczonego do użytkowania,

2. Ewidencja prowadzonych 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 w 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 Zleceniobiorca zidentyfikuje występujące problemy i ich przyczyny, opracuje rekomendacje działań i koniecznych zmian odnoszących się do zapewnienia zgodności działania Zleceniodawcy z wymaganiami Krajowych Ram Interoperacyjności.

V. Wymagane rezultaty audytu

Zleceniobiorca 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 Zleceniodawcy.

5. Zalecenia dotyczących sposobów, metod i środków usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyka. Lista poprawek do zainstalowania oraz szczegółowy opis zalecanych zmian konfiguracji.

6. Przygotowaną przez Zleceniobiorca aktualizację i uzupełnienie zestawu dokumentów Polityki Bezpieczeństwa zgodną z aktualnie obowiązującymi aktami prawnymi. Dokumenty te Zleceniobiorca przygotuje w porozumieniu ze Zleceniodawcą, uwzględniając specyfikę działania i organizację pracy Zleceniodawcy.

7. Wszystkie dokumenty związane z przeprowadzonym audytem Zleceniobiorca dostarczy Zleceniodawcy w postaci wydruku w dwóch egzemplarzach lub w postaci elektronicznej.

8. Zleceniobiorca pisemnie zobowiąże się, że dokumenty te będzie traktował jako poufne i nie przekaże ani nie udostępni ich nikomu bez pisemnej zgody Zleceniodawcy.

9. Zleceniobiorca, z dniem zatwierdzenia przez Zleceniodawcę sprawozdania audytowego, przeniesie na Zleceniodawcę autorskie prawa majątkowe do sprawozdania audytowego na polach eksploatacji, obejmujących:

a) odtwarzanie,
b) 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,
c) przekazywanie,
d) przechowywanie,
e) wyświetlanie,
f) wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji,
g) tłumaczenie,

h) przystosowywanie,
i) zmiany układu lub jakiekolwiek inne zmiany.

§ 3

Sposób realizacji umowy

1. Strony zobowiązują się do ścisłej współpracy w dobrej wierze, w celu jak najpełniejszej i najsprawniejszej realizacji Usług.

2. W celu realizacji Usług Zleceniodawca zobowiązuje się do niezwłocznego przekazywania Zleceniobiorcy wszelkich informacji/dokumentacji/urządzeń niezbędnych do wykonywania Usług.

3. Zleceniodawca odpowiada za przekazanie Zleceniobiorcy wszelkich informacji/dokumentacji/urządzeń niezbędnych do wykonywania Usług oraz stworzenie mu warunków do jej wykonania.

4. Zleceniodawca zobowiązuje się do niezwłocznego informowania Zleceniobiorcy o wszelkich znanych mu okolicznościach, które mogą mieć wpływ na realizację zobowiązań Zleceniobiorcy wynikających z niniejszej Umowy.

§ 4

Poufność i dane osobowe

1. Przy wykonywaniu Usług Zleceniobiorca i osoby przy pomocy których świadczy Usługi na rzecz Zleceniodawcy, zobowiązani są do zachowania w tajemnicy wszelkich informacji dotyczących Zleceniodawcy, w szczególności tych, które stanowią tajemnicę przedsiębiorstwa.
2. Zobowiązanie do zachowania poufności obowiązuje w okresie trwania Umowy oraz po jej wygaśnięciu.
3. W związku z faktem, że przy wykonywaniu Usług Zleceniobiorca może uzyskać dostęp do informacji stanowiących dane osobowe przetwarzane przez Zleceniodawcę, Zleceniodawca wyraża zgodę na ich przetwarzanie przez Zleceniobiorcę w celu wykonywania Umowy oraz zapewnia, że przetwarzanie danych osobowych w tym zakresie przez Zleceniobiorcę nie narusza jakichkolwiek praw Zleceniodawcy i osób, których te dane dotyczą.

§ 5

Termin realizacji i obowiązywania Umowy

1. Zleceniobiorca zobowiązuje się do realizacji przedmiotu umowy w terminie do dnia ..... 2019 roku,
2. W terminie wskazanym w ust. 1 Zleceniobiorca sporządzi także i przekaż Zleceniodawcy pisemny raport z audytu oraz przedstawi rekomendacje rozwiązań.

§ 6

Wynagrodzenie Zleceniobiorcy

1. Z tytułu należytego wykonania przedmiotu umowy Zleceniodawca zapłaci Zleceniobiorcy wynagrodzenie w wysokości ..... złotych netto (słownie: .....) powiększone o obowiązującą stawkę podatku VAT, tj. kwotę w wysokości ..... złotych (słownie: .....).

2. Wynagrodzenie będzie płatne na podstawie faktury VAT, wystawionej w ostatnim dniu miesiąca, w którym przekazano raport oraz rekomendację rozwiązań z przeprowadzonego audytu, o którym mowa w § 2.

3. Wynagrodzenie jest płatne przelewem na rachunek bankowy Zleceniobiorcy wskazany w fakturze VAT, w terminie 14 dni od dnia jej doręczenia Zleceniodawcy.

§ 7

Kary umowne

1. Strony ustalają odpowiedzialność za niewykonanie lub nienależyte wykonanie umowy w formie kar umownych.
2. Zleceniobiorca zapłaci Zleceniodawcy kary umowne za:
    1) rozwiązanie umowy przez Zleceniodawcę z winy Zleceniobiorcy – wysokość 10% łącznego wynagrodzenia umownego brutto, o którym mowa w paragrafie 6 ust. 1 umowy.
    2) za opóźnienie w wykonaniu przedmiotu umowy w wysokości 5% łącznego wynagrodzenia umownego brutto, o którym mowa w paragrafie 6 ust. 1 umowy za każdy dzień opóźnienia.

§ 8

Wzajemna komunikacja

1. Strony ustalają, że będą się komunikować osobiście, za pośrednictwem telefonów (połączenia głosowe, wiadomości sms lub multimedialne), oraz środków komunikacji elektronicznej, w szczególności poczty elektronicznej.

2. Każda ze Stron oświadcza, że pozostaje dostępna pod zawartymi w umowie danymi kontaktowymi (telefony, adresy e – mail) i będzie starała się na bieżąco, bez zbędnej zwłoki odpowiadać na kontakt drugiej ze Stron.

3. Osobą odpowiedzialną za realizację Umowy z ramienia Zleceniobiorcy jest ..... (email: ....., tel. .....).

4. Osobami odpowiedzialnymi za realizację Umowy z ramienia Zleceniodawcy jest: Pan Piotr Bąk dostępny pod adresem e – mail: pbak@otwock.pl

§ 9

W ramach wynagrodzenia, o którym mowa w paragrafie 6 ust. 1 niniejszej umowy Zleceniobiorca przenosi na Zleceniodawcę autorskie prawa majątkowe, w tym prawa zależne na wszelkich polach eksploatacji.

§ 10

Postanowienia końcowe

1. W sprawach nieuregulowanych Umową mają zastosowanie przepisy Kodeksu Cywilnego.

2. Integralną część Umowy stanowi Załącznik nr 1 – oferta z dnia ..... roku.

3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej
ze Stron.

4. Wszelkie zmiany Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.

5. Wszelkie spory jakie mogą wyniknąć z realizacji niniejszej Umowy, Strony poddają pod rozstrzygnięcie właściwych sądów powszechnych.

6. Wszelkie spory związane z zawarciem i realizacją Umowy podlegają prawu polskiemu.

ADWOKAT
Jarosław Dąbrowski

ZLECENIODAWCA **ZLECENIOBIORCA**