Toruń, dn. 19.08.2024

Urząd Miasta Torunia
Biuro Projektów Informatycznych
ul. Wały gen. Sikorskiego 10
e-mail: zp_bpi@um.torun.pl

syg. BPI.271.4342024

--- Wg. rozdzielnika ---

W ramach badania rynku

nr BPI/C/55/2024

Biuro Projektów Informatycznych
87-100 Toruń
ul. Wały gen. Sikorskiego 10

zwraca się z uprzejmą prośbą o przesłanie w trybie badania rynku propozycji cenowej na:

usługa audytu bezpieczeństwa oraz opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001, Krajowymi Ramy Interoperacyjności, Ogólnym rozporządzeniem o ochronie danych oraz Dyrektywą NIS2 zgodnie z załączoną specyfikacją

1. Proszę podać ryczałtową cenę **netto i brutto w złotych dla każdej licencji z osobna**
2. Miejsce składania ofert: Ofertę proszę dostarczyć do Biura Projektów Informatycznych UMT ul. Wały gen. Sikorskiego 10, pok.23 osobiście, lub na adres e-mail (np. w formacie PDF): zp_bpi@um.torun.pl
3. Termin składania ofert: do **26.08.2024r. do godz. 12:00 (decyduje godzina otrzymania oferty przez Zamawiającego)**
4. Wymagania i warunki Zamawiającego:
   a) W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Oferentami w celu uzupełnienia lub doprecyzowania ofert.
   b) Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy pisemnej.
   c) Oferty złożone po terminie nie zostaną rozpatrzone.
5. Niniejsza oferta nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych.
6. Zaproszenie nie jest postępowaniem o udzielenie zamówienia publicznego w rozumieniu przepisów Prawa zamówień publicznych oraz nie kształtuje zobowiązania Zamawiającego do przyjęcia którejkolwiek z ofert.
7. **Zaproszenie ma na celu dokonanie oszacowania wartości zamówienia publicznego zgodnie z Zarządzeniem nr 247 PMT z dnia 22.09.2021r.**

Główny Specjalista
Grzegorz Hrynek

Załącznik 1

PRZEDMIOT ZAMÓWIENIA	Audyty .....
ZAMAWIAJĄCY	Gmina Miasta Toruń - wydział prowadzący – Biuro Projektów Informatycznych UMT .....
WYKONAWCA **Adres** **Numer telefonu / fax** **Internet http: //** **e-mail**	
Kryterium 1. CENA OFERTY NETTO / BRUTTO (z obowiązującym podatkiem VAT)	Cyfrowo netto: ..... Cyfrowo brutto: ..... Słownie brutto: .....
Data **Podpis**	

Specyfikacja Istotnych Warunków Zamówienia (SIWZ)

1. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest usługa audytu bezpieczeństwa oraz opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001, Krajowymi Ramy Interoperacyjności, Ogólnym rozporządzeniem o ochronie danych oraz Dyrektywą NIS2.

2. Zakres usługi obejmuje

Przeprowadzenie audytów, sporządzenie planu minimalizacji ryzyka, opracowanie dokumentacji Systemu Zarządzenia Bezpieczeństwa Informacji oraz szkolenia dla pracowników i kadry zarządzającej.

3. Audyt bezpieczeństwa informacji - audyt techniczny obejmujący co najmniej:
   a) Inwentaryzacja oprogramowania i zasobów sprzętowych w zakresie posiadania:
      i. Ewidencji oprogramowania dopuszczonego do użytkowania i jego klasyfikacja z punktu widzenia wymogów w zakresie cyberbezpieczeństwa (co do zabezpieczeń i dokumentacji bezpieczeństwa jaka powinna być dla niego stworzona),
      ii. Ewidencji prowadzonych kontroli w zakresie legalności oprogramowania instalowanego na stacjach roboczych,
      iii. Zasady zarządzania oprogramowaniem,
      iv. Procedur zapewnienie bezpieczeństwa danych przy dokonywaniu napraw sprzętu i oprogramowania,
      v. Formalnegowyznaczenia osób uprawnionych do dokonywania napraw sprzętu i oprogramowania,
      vi. Procedur obsługi komputerów oraz pracy w sieci,
      vii. Inwentaryzacji sprzętu działającego w infrastrukturze informatycznej,
      viii. Inwentaryzacji usług sieciowych z opisem wzajemnych zależności tych usług,
      ix. Inwentaryzacji baz danych ze wskazaniem aplikacji korzystających z tych baz,
      x. Inwentaryzacji używanych aplikacji ze wskazaniem administratorów tych aplikacji,
      xi. Procedur Zarządzania aplikacjami (wykaz licencji i aplikacji, zasady dostępu do aplikacji, monitorowanie instalacji oprogramowania oraz osoby nadzorujące),
      xii. Fizycznego zabezpieczenia obszarów przetwarzania danych,
      xiii. Zabezpieczenie i wyposażenie serwerowni,
      xiv. Pozostałych procedur i rejestrów wymaganych regulacjami wskazanymi w opisie przedmiotu zamówienia oraz dobrymi praktykami
   b) Audyt bezpieczeństwa, wydajności i podatności infrastruktury informatycznej obejmujący co najmniej:
      i. Weryfikację istniejących procedur zarządzania systemami teleinformatycznymi,
      ii. ,
      iii. Weryfikację poprawności aktualizacji systemu informatycznego,
      iv. Weryfikację poprawności aktualizacji zabezpieczeń antywirusowych,
      v. Weryfikację zabezpieczeń fizycznych, zasilania awaryjnego (testy, szkolenia użytkowników),
      vi. Weryfikację bezpieczeństwa okablowania strukturalnego,
      vii. Weryfikację systemów chłodzenia,
      viii. Weryfikację systemów alarmowych,
      ix. Sprawdzenie wyposażenia i zabezpieczenia pomieszczeń serwerowni,
      x. Weryfikacjęwykonywania i sprawdzania kopii zapasowych (częstotliwość wykonywania, miejsce przechowywania, osoby odpowiedzialne),
      xi. Zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji,
      xii. Procedury postępowania w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych,

xiii. Dokumentowania konfiguracji systemów służących przetwarzaniu danych osobowych,
xiv. Stosowania mechanizmów kryptograficznych i ich adekwatność do zagrożeń i wymogów prawa,
xv. Urządzenia sieciowe,
xvi. Pozostałych zasad wymaganych regulacjami wskazanymi w opisie przedmiotu zamówienia oraz dobrymi praktykami.

c) Weryfikacja podatności systemu informatycznego na ingerencje ze strony osób trzecich:
   i. przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz mających na celu zidentyfikowanie podatności na włamanie,
   ii. przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz sieci Zamawiającego,
   iii. eksploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet,
   iv. eksploitacja dostępnych urządzeń oraz usług w sieci wewnętrznej,
   v. skanowanie portów TCP/UDP i próba wykrycia usług sieciowych,
   vi. skanowanie hostów aktywnych w sieci,
   vii. weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,
   viii. weryfikacja ochrony przed szkodliwym oprogramowaniem,
   ix. weryfikacja procedur związanych z rejestracją błędów,
   x. weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania.
d) Sprawdzenie podatności serwisów internetowych,
e) Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych,
f) Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego zdalnego (przez WWW) dostępu do paneli administracyjnych,
g) Posiadanego zabezpieczenia logicznego na styku sieci lokalnej z Internetem,
h) Sporządzenie raportu, w którym zamieszczone zostaną informacje czytelne zarówno dla kierownictwa jak i administratorów systemów informatycznych. Raport będzie obejmował informacje o wykrytych niezgodnościach sposobu zarządzania bezpieczeństwem informacji z wymaganiami cyberbezpieczeństwa oraz wyniki badań technicznych (poszczególne podatności) wraz rekomendacjami służącymi do ich samodzielnego wyeliminowania.
i) Przygotowanie procedur oraz polityk regulujących działania w obszarach, w których obowiązujące obecnie procedury są niewystarczające.

4. Audyt bezpieczeństwa przetwarzania informacji – Audyt organizacyjny – przygotowanie dokumentacji obejmujący co najmniej:

a) Audyt organizacyjny,
b) Określenie istotnych danych i istotnych zasobów informatycznych,
c) Weryfikacja spełnienia wymagań regulacji polskich oraz wynikających z dyrektyw i rozporządzeń UE,
d) Regulacje w obszarze zarządzania bezpieczeństwem informacji, plany awaryjne,
e) Procedury reagowania na incydenty,
f) Pozostałe obszary wymagane regulacjami wskazanymi w opisie przedmiotu zamówienia oraz dobrymi praktykami,
g) Sporządzenie raportu, w którym zamieszczone zostanie posumowanie audytu oraz rekomendacje dotyczące sposobu podniesienie bezpieczeństwa przetwarzania informacji.
h) Opracowanie dokumentacji Systemu Zarządzenia Bezpieczeństwa Informacji:
   I. Zakres systemu zarządzania bezpieczeństwem informacji,

II. Księga systemu zarządzania bezpieczeństwem informacji,
III. Polityka bezpieczeństwa informacji,
IV. Schemat organizacyjny zarządzania bezpieczeństwem informacji,
V. Deklaracja stosowania dla systemu bezpieczeństwa informacji,
VI. Plan kontynuacji działania,
VII. Metodyka szacowania ryzyka,
VIII. Instrukcje i Procedury:
    i. Nadzór nad dokumentami,
    ii. Działania korekcyjne i zapobiegawcze,
    iii. Audyty wewnętrzne,
    iv. Nadzór nad zapisami,
    v. Przegląd zarządzania,
    vi. Zarządzanie incydentami,
    vii. Bezpieczeństwo wewnętrzne organizacji,
    viii. Ewakuacja personelu i sprzętu,
    ix. Klasyfikacja informacji,
    x. Ocena ryzyk generowanych przez strony zewnętrzne,
    xi. Postępowanie w przypadku odejścia pracownika,
    xii. Bezpieczeństwo infrastruktury teleinformatycznej,
    xiii. Bezpieczeństwo fizyczne,
    xiv. Nadzór nad przyrządami pomiarowymi.
IX. Sporządzenie pozostałej dokumentacji której brak stwierdzono w trakcie audytów opisanych w punktach 3 i 4 oraz pozostałych wymaganych regulacjami wskazanymi w opisie przedmiotu zamówienia oraz dobrymi praktykami.

5. Sporządzenie planu minimalizacji ryzyka poprzedzone przeprowadzeniem analizy ryzyka:
a) Identyfikacja aktywów,
b) Ocena podatności i skutków utraty poufności, integralności i dostępności,
c) Ocena ryzyka zgodnie z wybraną metodyką,
d) Sporządzenie planu minimalizacji ryzyka.
6. Szkolenie personelu w zakresie:
a) podstawowych wymagań normy ISO/IEC 27001, Krajowych Ramy Interoperacyjności, Ogólnego rozporządzenia o ochronie danych oraz Dyrektywy NIS2,
b) Dokumentacji Systemu Zarządzenia Bezpieczeństwa Informacji.
7. Wymagania w stosunku do wykonawcy:
a) Wykonawca winien wykazać, że dysponuje lub będzie dysponować osobami pełniącymi następujące funkcje i posiadającymi wskazane doświadczenie i kwalifikacje:
    i. Ekspert ds. Audytu bezpieczeństwa (co najmniej 2 osoby), który spełnia następujące wymagania:
        I. posiada co najmniej 3-letnie doświadczenie w zakresie przeprowadzania audytów bezpieczeństwa informacji w projekcie informatycznym
        II. posiada wykształcenie wyższe,
        III. posiada aktualny certyfikat Audytora Wiodącego norm ISO 27001 lub certyfikat równoważny opisany w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
b) Wykonawca winien wykazać, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, należycie wykonał:
    i. co najmniej 1 usługę polegającą na przeprowadzeniu audytu bezpieczeństwa informacji o wartości co najmniej 30000 zł brutto (słownie: trzydzieści tysięcy złotych brutto),

ii. co najmniej 1 usługę, polegającą na przeprowadzeniu audytu bezpieczeństwa, z zastosowaniem testów penetracyjnych oraz analizy implementacji mechanizmów
iii. bezpieczeństwa w projekcie informatycznym o wartości co najmniej 30000 zł brutto (słownie: trzydzieści tysięcy złotych brutto),
iv. co najmniej 1 usługę o wartości usługi co najmniej 10000 zł brutto (słownie: dziesięć tysięcy złotych brutto) polegającą na realizacji projektu polegającego na wdrożeniu systemu informatycznego.

8. Oferta podzielona na 4 etapy (ceny brutto)- płatność po zamknięcie każdego z etapów. Oferta na całość:
    a. Audyt bezpieczeństwa informacji- audyt techniczny,
    b. Audyt bezpieczeństwa przetwarzania informacji – Audyt organizacyjny – przygotowanie dokumentacji,
    c. Sporządzenie planu minimalizacji ryzyka poprzedzone przeprowadzeniem analizy ryzyka,
    d. Szkolenie personelu.