Opis przedmiotu zamówienia

I. PRZEDMIOT ZAMÓWIENIA:

Wykonanie audytu bezpieczeństwa informacji w **Urzędzie Miasta Gostynina** zgodnego z wymogami § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017 poz. 2247) oraz Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U.2016 poz. 922 z późn. zm.) w oparciu o wymagania normę ISO 27001

Liczba pracowników: 76

Liczba lokalizacji: 3

Liczba serwerów: 3

Liczba stacji roboczych: 80

Szczegółowy zakres audytu:

1. Audyt bezpieczeństwa informacji we wszystkich obszarach funkcjonowania organizacji

a. Audyt organizacyjny

- Regulacje w obszarze zarządzania bezpieczeństwem informacji;
- Odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji.

b. Audyt fizyczny i środowiskowy

- Weryfikacja granic obszaru bezpiecznego;
- Weryfikacja zabezpieczeń wejścia/wyjścia;
- Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;
- Weryfikacja bezpieczeństwa okablowania strukturalnego;

c. Audyt teleinformatyczny

- Przeprowadzenie testów penetracyjnych systemu informatycznego wewnętrznie i zewnętrznie, określenie luk, wskazanie rozwiązań naprawczych, opracowanie raportu
- Weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi;
- Przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania ciągłości działania;

- Weryfikacja ochrony przed oprogramowaniem szkodliwym;
- Weryfikacja procedur zarządzania kopiami zapasowymi;
- Weryfikacja procedur związanych z rejestracją błędów;
- Weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
- Weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
- Weryfikacja zabezpieczeń nośników wymiennych
- Weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);

d. Audyt socjotechniczny

- Przeprowadzenie wyrywkowych testów socjotechnicznych w fizycznej lokalizacji zamawiającego oraz za pośrednictwem telefonu i poczty elektronicznej
- Sporządzenie raportu wraz z zaleceniami naprawczymi

2. Audyt ochrony danych osobowych – odniesienia do zmian RODO, UODO, oraz zmian ABI i IODO:

a. Aktualizacja i dostosowanie Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym wraz z procedurami uzupełniającymi do RODO

b. Opracowanie dokumentacji do zaimplementowania wymaganej zgodnie z nowymi przepisami RODO i UODO, w tym:

- Klauzule zgód na przetwarzanie danych osobowych;
- Obowiązek informacyjny (klauzule);
- Wzory umów powierzenia przetwarzania danych osobowych;
- Rejestr czynności przetwarzania danych osobowych;
- Analiza ryzyka.

c. Szkolenie poaudytowe dla wszystkich pracowników z zakresu bezpieczeństwa pracy w systemach teleinformatycznych, oraz z zakresu ochrony danych osobowych.

2. Zapewnienie opieki doradczej po zakończeniu audytu – konsultacje zamawiającego z wykonawcą zaleceń zawartych w raportach przez okres 12 miesięcy od zakończenia audytu w ramach wynagrodzenia wskazanego w umowie.

III. WARUNKI UDZIAŁU W POSTĘPOWANIU

W postępowaniu może wziąć udział Wykonawca, który dysponuje zespołem minimum trzech specjalistów z kwalifikacjami popartymi posiadaniem certyfikatów niżej wyszczególnionych.

- Minimum dwie osoby z zespołu posiadać muszą certyfikat audytora wewnętrznego SZBI wg ISO27001, trzecia z tych osób - certyfikat audytora wiodącego SZBI wg ISO27001.

- Zespół audytorów musi udokumentować łącznie stosownymi certyfikatami posiadanie wiedzy z zakresu

- ochrony danych osobowych,

- analizy ryzyka,

- przeprowadzenia analizy bezpieczeństwa w kontekście rozporządzenia KRI oraz umiejętności opracowania stosownej dokumentacji SZBI dla urzędu

- Wykonawca musi posiadać doświadczenie w przeprowadzaniu co najmniej 3 audytów bezpieczeństwa informacji w ciągu 3 lat w urzędach administracji publicznej lub jednostkach samorządu terytorialnego.

- W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z formularzem oferty: certyfikatów oraz wykazu zrealizowanych audytów bezpieczeństwa informacji w urzędach administracji publicznej lub jednostkach samorządu terytorialnego.

- Oferta musi zawierać nazwę wykonawcy, siedzibę wykonawcy, certyfikaty potwierdzające kwalifikacje wykonawcy, oraz cenę za usługę.

Zamówienie należy wykonać do dnia 18 maja 2018 r.