OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zaprojektowanie i wdrożenie Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001:2014, w Instytucie „Centrum Zdrowia Matki Polki" w Łodzi.

I. KONTEKST, ZAŁOŻENIA DOTYCZĄCE ZAMÓWIENIA

1. Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Zamawiającego poprzez wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami ujętymi w: PN-ISO/IEC 27002:2014, PN-ISO/IEC 27005:2014, PN-ISO/IEC 24762:2010, PN-ISO/IEC 22301 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, dalej: „KSC".
2. Informacje ogólne o środowisku Zamawiającego:
   a) Przetwarzanie informacji odbywa się w **1 jednostce** organizacyjnej. Informacje przetwarzane są w formie papierowej oraz systemach informatycznych. Zamawiający zatrudnia około 2700 osób.
   b) Środowisko teleinformatyczne zawiera obecnie około 50 elementów aktywnych sieci i około 40 serwerów fizycznych 60 wirtualnych.
3. Zamawiający w ciągu 14 dni od dnia zawarcia Umowy przekaże Wykonawcy dokumenty, którymi dysponuje w obszarze związanym z bezpieczeństwem informacji, w tym procedury wewnętrzne i wyniki przeprowadzonych audytów oraz szczegółową strukturę organizacyjną i informacje o środowisku teleinformatycznym, niezbędne do opracowania przez Wykonawcę wstępnego harmonogramu prac.

II. ZAKRES ZAMÓWIENIA

Usługa zaprojektowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (w skrócie SZBI) będzie obejmować swoim zakresem:

- etap I - audyt przedwdrożeniowy u Zamawiającego;
- etap II - klasyfikacja informacji przetwarzanych u Zamawiającego;
- etap III - szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014;
- etap IV - opracowanie dokumentacji SZBI;
- etap V – audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej

1. Audyt przedwdrożeniowy

Audyt przedwdrożeniowy ma na celu weryfikację poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2014 przez Zamawiającego, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych u Zamawiającego, w obszarach określonych załącznikiem A do ww. normy, tj.:

- Polityki bezpieczeństwa informacji (A.5);
- Organizacja bezpieczeństwa informacji (A.6);
- Bezpieczeństwo zasobów ludzkich (A.7);
- Zarządzanie aktywami (A.8);
- Kontrola dostępu (A.9);
- Kryptografia (A10); − Bezpieczeństwo fizyczne i środowiskowe (A.11);

- Bezpieczna eksploatacja (A.12);
- Bezpieczeństwo komunikacji (A.13)
- Pozyskiwanie, rozwój i utrzymanie systemów (A.14);
- Relacje z dostawcami (A.15);
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji (A.16);
- Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania (A.17);
- Zgodność (A.18).
-

2. Klasyfikacja informacji przetwarzanych u Zamawiającego

W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:

- opracowanie metodyki klasyfikowania informacji przetwarzanych u Zamawiającego;
- opracowanie modelu podziału informacji przetwarzanych u Zamawiającego w zależności od poziomu ich wrażliwości i przeznaczenia;
- sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych u Zamawiającego;
- opracowanie raportu z procesu klasyfikacji informacji.

3. Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014

W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego, a w szczególności:

- opracować metodykę szacowania ryzyka spełniającą wymagania PN-ISO/IEC 27005:2014, optymalną ze względu na charakter działalności Zamawiającego;
- opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
- przeprowadzić wspólnie z wyznaczonymi pracownikami Zamawiającego proces szacowania ryzyka, w tym:
    - zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
    - opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Zamawiającego;
    - opracować przy współudziale wyznaczonych pracowników Zamawiającego plan postępowania z ryzykiem.

4. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

Opracowanie wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami:

a) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070),

b) 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. z 2017 r. poz. 2247),
c) ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655).

Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest opracować i przedstawić koncepcję wdrożenia Polityki Bezpieczeństwa Informacji u Zamawiającego zawierającą mapę dokumentów SZBI, stanowiącą szczegółowy wykaz dokumentów SZBI z zaznaczeniem ich wzajemnych powiązań, w tym:

- Dokument Główny Polityki Zarządzania Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;
- Deklarację Stosowania
- Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji u Zamawiającego w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;
- Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

5. Audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej

Przeprowadzenie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w Instytucie „Centrum Zdrowia Matki Polki" w Łodzi, uznanego decyzją Ministra Zdrowia, za Operatora Usługi Kluczowej, zgodnie z ustawą KSC.

Audyt zostanie przeprowadzony zgodnie z postanowieniami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przez co najmniej dwóch audytorów posiadających certyfikaty określone w przepisach wydanych na podstawie art. 15 ust. 8) ww. ustawy, tj. m.in. 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 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób.

Wykonawca przy wykonywaniu umowy może oprócz audytorów wskazanych w ust. 1 dodatkowo posiłkować się innymi pracownikami i współpracownikami Wykonawcy, w szczególności informatykami i prawnikami.

Powierzenie wykonania części przedmiotu Umowy innym pracownikom i współpracownikom nie wymaga uprzedniej zgody Szpitala, przy czym Wykonawca odpowiada za działania osób trzecich jak za działania własne.

Po zakończeniu audytu Wykonawca przygotuje i przekaże Szpitalowi w formie elektronicznej oraz papierowej sprawozdanie z przeprowadzonego audytu.

Wymagania

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 24 ust. 1 pkt 12-23 oraz art. 24 ust. 5 pkt 1 PZP.

Zamawiający określa warunki udziału w postępowaniu, dotyczące zdolności zawodowej lub technicznej oraz sytuacji ekonomicznej Wykonawcy, które umożliwią realizację zamówienia na poziomie jakości, oczekiwanym przez Zamawiającego, a mianowicie:

1. Należyte wykonanie w okresie ostatnich trzech lat przed upływem terminu składania ofert co najmniej:
    a. 2 usług polegających na przygotowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji, w skład którego wchodzi kompletna dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji, każda ww. usługa o wartości nie mniejszej niż 30.000 - 50 000 PLN brutto, w tym jedna usługa zrealizowana na rzecz podmiotu administracji publicznej; oraz
    b. posiadać doświadczenie w zakresie szacowania ryzyka wystąpienia incydentu oraz obsługi incydentu w obszarze bezpieczeństwa informacji w podmiocie wykonujących działalność leczniczą, zatrudniającym co najmniej 400 osób, przez okres co najmniej 60 miesięcy;
    c. posiadać doświadczenie w pełnieniu funkcji Osoby wyznaczonej do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa w podmiocie wykonujących działalność leczniczą, zatrudniającym co najmniej 400 osób, przez okres co najmniej 12 miesięcy.

2. Audyt bezpieczeństwa może być przeprowadzony przez:
    1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
    2) co najmniej dwóch audytorów posiadających:
        a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
        b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
        c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.
    3) Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

a) Certified Internal Auditor (CIA);

b) Certified Information System Auditor (CISA);
c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN
d) 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,* w zakresie certyfikacji osób;
e) 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;
f) Certified Information Security Manager (CISM);
g) Certified in Risk and Information Systems Control (CRISC);
h) Certified in the Governance of Enterprise IT (CGEIT);
i) Certified Information Systems Security Professional (CISSP);
j) Systems Security Certified Practitioner (SSCP);
k) Certified Reliability Professional;
l) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.