Opis Przedmiotu Zamówienia

§1
Przedmiot zamówienia

Przeprowadzenie audytu zgodnego z wymaganiami Krajowych Ram Interoperacyjności (KRI) dla systemów teleinformatycznych oraz procesów zarządzania bezpieczeństwem informacji w Urzędzie, zgodnie z rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych, wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773, dalej rozporządzenie KRI). Wsparcie merytoryczne po audytowe w ilości 40 godzin roboczych w celu dostosowania Urzędu do wymagań KRI.

§2
Cel audytu

Celem audytu jest weryfikacja zgodności systemów teleinformatycznych, procedur i procesów zarządzania bezpieczeństwem informacji w Urzędzie z obowiązującymi przepisami określonymi w rozporządzeniu KRI. Szczegółowym celem audytu jest:

1. Identyfikacja potencjalnych niezgodności z wymaganiami rozporządzenia KRI.
2. Ocena wdrożonych środków technicznych i organizacyjnych w zakresie bezpieczeństwa systemów teleinformatycznych i ochrony danych.
3. Przegląd i ocena polityki bezpieczeństwa, analizy ryzyka oraz zarządzania incydentami i ciągłością działania.
4. Ocena zgodności systemów Urzędu z wymogami minimalnych standardów technicznych i organizacyjnych dotyczących interoperacyjności.

§3
Zakres audytu

Audyt obejmuje następujące obszary:

1. Zgodność z minimalnymi wymaganiami KRI dla systemów teleinformatycznych:
    a. Sprawdzenie, czy systemy informatyczne Urzędu spełniają minimalne wymogi w zakresie bezpieczeństwa, ochrony danych oraz zarządzania dostępem.
    b. Ocena wdrożonych mechanizmów kontrolnych, takich jak zabezpieczenia przed nieautoryzowanym dostępem, ochrona danych, kontrola dostępu, szyfrowanie danych oraz monitorowanie systemów.
2. Zgodność z minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji:
    a. Weryfikacja, czy rejestry publiczne prowadzone przez Urząd są zgodne z wymogami interoperacyjności oraz czy proces wymiany informacji jest zgodny z obowiązującymi standardami.
    b. Ocena bezpieczeństwa komunikacji między systemami, w tym wykorzystywanych protokołów i metod zabezpieczających.
3. Polityka bezpieczeństwa informacji:
    a. Ocena zgodności wdrożonej polityki bezpieczeństwa informacji z KRI.
    b. Sprawdzenie procedur dotyczących zarządzania dostępem, ochrony danych oraz monitorowania i wykrywania incydentów.
4. Analiza ryzyka:
    a. Weryfikacja, czy Urząd regularnie przeprowadza analizę ryzyka dotyczącą systemów teleinformatycznych oraz bezpieczeństwa informacji.
    b. Sprawdzenie dokumentacji analizy ryzyka oraz ocena skuteczności działań zaradczych.
5. Zarządzanie incydentami bezpieczeństwa:

   a. Ocena procedur zarządzania incydentami bezpieczeństwa w Urzędzie, w tym wykrywania, zgłaszania i reagowania na incydenty.
   b. Przegląd procesów eskalacji oraz raportowania incydentów do odpowiednich organów.
6. Zarządzanie ciągłością działania:
   a. Weryfikacja, czy Urząd posiada plany ciągłości działania (BCP) oraz procedury awaryjne w przypadku wystąpienia incydentów lub awarii systemów.
   b. Sprawdzenie, czy plany te są regularnie testowane oraz aktualizowane w zależności od zmian w środowisku systemów teleinformatycznych.
7. Szkolenia i świadomość pracowników:
   a. Ocena, czy Urząd organizuje regularne szkolenia dla pracowników dotyczące bezpieczeństwa informacji oraz zasad postępowania w sytuacjach incydentów.
8. Ochrona danych osobowych:
   a. Sprawdzenie zgodności z przepisami dotyczącymi ochrony danych osobowych, w tym wdrożonych środków technicznych i organizacyjnych mających na celu ochronę danych osobowych przetwarzanych w Urzędzie.

§4

Zakres dodatkowy do realizacji

1. Po przeprowadzeniu audytu, Wykonawca przekaże Zamawiającemu raport z audytu, który będzie zawierał:
   a. Szczegółowy opis stanu bezpieczeństwa systemów informatycznych oraz ich zgodności z wymogami KRI.
   b. Wskazanie zidentyfikowanych niezgodności oraz luk w systemach bezpieczeństwa informacji.
   c. Rekomendacje dotyczące działań naprawczych mających na celu dostosowanie Urzędu do wymogów KRI.
   d. Opis kroków, jakie Zamawiający powinien podjąć, aby osiągnąć pełną zgodność z KRI, w tym wskazanie niezbędnych działań technicznych i organizacyjnych
2. W ramach godzin konsultacyjnych firma zapewni wsparcie w wykonaniu analizy ryzyka dla systemów teleinformatycznych i procesów:
   a. Firma audytorska zapewni wsparcie merytoryczne dla przeprowadzenia kompleksowej analizy ryzyka, która obejmie identyfikację zagrożeń związanych z funkcjonowaniem systemów teleinformatycznych, ochroną danych oraz zgodnością z KRI.
   b. Analiza ryzyka będzie oparta na standardach ISO 31000 oraz ISO/IEC 27005, które określają metodologie oceny ryzyka w kontekście zarządzania bezpieczeństwem informacji.
   c. Wyniki analizy ryzyka będą stanowiły podstawę do opracowania planu zarządzania ryzykiem, zawierającego rekomendacje dotyczące działań minimalizujących ryzyko w kluczowych obszarach.
   d. Zostaną ocenione możliwe skutki potencjalnych incydentów (w tym incydentów związanych z bezpieczeństwem danych) oraz prawdopodobieństwo ich wystąpienia, a także sposoby zarządzania tymi ryzykami.
3. W ramach godzin konsultacyjnych firma zapewni wsparcie w wykonaniu Planu Ciągłości Działania (PCD) zgodny z normami ISO 22301, który będzie określał procedury na wypadek awarii systemów IT, incydentów związanych z bezpieczeństwem danych oraz innych zdarzeń kryzysowych, które mogą zakłócić działalność instytucji. Plan Ciągłości Działania będzie zawierał szczegółowe instrukcje dotyczące:
   a. Przywracania kluczowych funkcji systemów teleinformatycznych w sytuacjach kryzysowych.

b. Zapewnienia minimalnej funkcjonalności systemów informatycznych w przypadku awarii.
c. Określenia odpowiedzialności i roli poszczególnych członków zespołu ds. zarządzania kryzysowego.
d. W ramach godzin konsultacyjnych firma zapewni wsparcie w wykonaniu opracowaniu planu przywracania systemów (Disaster Recovery Plan - DRP):
a. Firma zapewni wsparcie w przygotowaniu szczegółowego Planu Odtwarzania Systemów w przypadku incydentów krytycznych, który będzie obejmował techniczne aspekty przywracania działania systemów teleinformatycznych po awarii, zgodnie z najlepszymi praktykami branżowymi.
b. DRP będzie zawierał wytyczne dotyczące:
i. Zabezpieczenia i odtwarzania danych po awarii.
ii. Testowania i regularnej aktualizacji planu, aby zapewnić jego skuteczność.
e. W ramach godzin konsultacyjnych firma zapewni wsparcie w wykonaniu procedury testowania Planów Ciągłości Działania i Odtwarzania Systemów. Regularne testy tych planów będą przeprowadzane w celu ich weryfikacji i dostosowania do zmieniających się warunków technicznych i organizacyjnych.

§5

Wsparcie merytoryczne po audycie / Godziny konsultacyjne.

1. Wykonawca zapewni wsparcie merytoryczne dla Zamawiającego przez 40 godzin w okresie 3 miesięcy od odebrania wyników audytu. Wsparcie obejmuje:
   a. Pomoc w wykonaniu Analizy ryzyka zgodnej z KRI.
   b. Wsparcie w opracowaniu Planu Ciągłości Działania (BCP).
   c. Pomoc w opracowaniu Planu Odtworzenia po awarii (DRP).
   d. Dostosowanie dokumentacji Polityki Bezpieczeństwa
2. Stawka za roboczo-godzinę wsparcia musi być znana i podana w ofercie.
3. Wsparcie będzie rozliczane na podstawie rzeczywistego wykorzystania roboczo-godzin. Zamawiający zgłasza zapotrzebowanie na wsparcie merytoryczne telefonicznie lub poprzez email. Wykonawca proponuje termin realizacji konsultacji z maksymalnie 2-dniowym czasem realizacji konsultacji. Wykonawca zobowiązuje się zorganizować spotkanie online (Teams) po wcześniejszym zaakceptowaniu terminu przez Zamawiającego. Dopuszczalne jest również wsparcie telefoniczne lub online tak zwane „od ręki” bez wcześniej umówionego terminu konsultacji.
4. Rozliczenie wsparcia odbywa się za pełne godziny – każda rozpoczęta godzina jest liczona jako pełna.
5. Wsparcie będzie dostępne od poniedziałku do piątku, w godzinach od 08:00 do 16:00.
6. Rozliczenie godzin wsparcia będzie odbywało się protokolarnie poprzez protokół odbioru po każdej konsultacji. Na podstawie protokołu Wykonawca będzie wystawiał fakturę VAT za liczbę godzin wskazaną w protokole.

§6

Wymagania wobec Wykonawcy

1. Wykonawca do realizacji audytu zapewni minimum dwóch audytorów , gdzie każdy będzie posiadać co najmniej jeden z certyfikatów potwierdzający kompetencje w zakresie audytów bezpieczeństwa informacji, takich jak CISA, CISSP, ISO/IEC 27001.
2. Każdy audytor będzie posiadał doświadczenie w przeprowadzaniu minimum 3 audytów zgodnych z KRI w jednostkach administracji publicznej.
3. Znajomość przepisów dotyczących ochrony danych osobowych (RODO) oraz wymogów Krajowych Ram Interoperacyjności.

4. Wykonawca musi posiadać doświadczenie w przeprowadzaniu audytów w instytucjach administracji publicznej.

§7

Wymagania dotyczące raportu z audytu

1. Raport końcowy z audytu powinien zawierać:
    a. Szczegółowy opis stanu bezpieczeństwa systemów informatycznych oraz zgodności z wymogami KRI.
    b. Wskazanie zidentyfikowanych niezgodności oraz luk w zakresie bezpieczeństwa.
    c. Rekomendacje działań naprawczych mających na celu dostosowanie Urzędu do wymogów KRI.
    d. Raport z analizy ryzyka oraz ocena procedur zarządzania incydentami bezpieczeństwa.

§8

Termin realizacji

1. Realizacja audytu wraz z przedstawieniem raportu końcowego powinna nastąpić w ciągu 30 dni roboczych od dnia podpisania umowy.
2. Usługa wsparcia merytorycznego w ilości 40 godzin w celu dostosowania Urzędu do KRI w ciągu 3 miesięcy od dnia realizacji audytu.

§9

Opis środowiska Zamawiającego

1. Główny Inspektorat Farmaceutyczny znajduje się na ulicy Senatorskiej 12 w Warszawie i jest to jedyna lokalizacja urzędu. Nie posiadamy dodatkowych lokalizacji.
2. Urząd posiada obecnie zatrudnione 183 osoby.
3. Dane dotyczące ilości komputerów, serwerów oraz innych urządzeń podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe, takie jak drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP itp.):
4. Ilość komputerów: 278
5. Ilość serwerów (fizycznych i wirtualnych): 54
6. Ilość pozostałych urządzeń:
    a. Access Point – 7 szt
    b. Telefon VoiP – 46 szt.
    c. Centrala telefoniczna – 1
    d. Drukarki - 81 szt.
    e. Switche zarządzalne – 15 szt.
    f. Switche niezarządzalne – 3 szt.
7. Zamawiający nie przewiduje wykonywania audytu ochrony danych osobowych w ramach postępowania.