

135575

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest **wykonanie audytu na zgodność z wymaganiami ustawy o Krajowym Systemie Cyberbezpieczeństwa**

Przedmiot zamówienia umowy zostanie wykonany w terminie 30 dni od dnia zawarcia Umowy, jednak nie później niż do dnia 01.12.2024 r.

Zamawiający jest Operatorem Usługi kluczowej w obszarze:

- 1. Zarządzania danymi epidemiologicznymi**
- 2. Gromadzenia i udostępniania Elektronicznej Dokumentacji Medycznej**

I. Zakres prac.

- 1) Analiza dokumentacji dotyczącej bezpieczeństwa IT;
- 2) Analiza skuteczności funkcjonowania mechanizmów kontrolnych;
- 3) Opracowanie raportu zawierającego opis zidentyfikowanych niezgodności oraz obserwacji wraz z rekomendacjami, w tym zalecanym harmonogramem i szacunkowym kosztem rekomendowanych zmian. Raport musi zostać sporządzony i przekazany Zamawiającemu w wersji elektronicznej w formacie PDF w postaci spakowanej i zaszyfrowanej, a hasło dostarczone odrębnym kanałem;
- 4) Opracowanie streszczenia raportu. Streszczenie raportu musi zostać sporządzone i przekazany Zamawiającemu w wersji elektronicznej w formacie PDF w postaci spakowanej i zaszyfrowanej, a hasło dostarczone odrębnym kanałem;
- 5) Przystawienie wyników analizy Kierownictwu organizacji w formie prezentacji podczas spotkania zamykającego.

II. Obszary analizy.

- 1) Obszar 1: Organizacja zarządzania bezpieczeństwem informacji
Zweryfikowanie zgodności z wymaganiami w zakresie stworzenia i utrzymywania systemu zarządzania zapewniającego zgodność z UKSC.
- 2) Obszar 2: Procesy zarządzania bezpieczeństwem informacji
Zweryfikowanie zgodności z wymaganiami bezpieczeństwa informacji w zakresie poprawności ich zdefiniowania, wdrożenia, eksploatacji i nadzorowania procesów zapewniających bezpieczeństwem informacji.
- 3) Obszar 3: Zarządzanie ryzykiem
Zweryfikowanie zgodności z wymaganiami w zakresie poprawności stosowanej metodyki zarządzania ryzykiem oraz kompletności procesu zarządzania.
- 4) Obszar 4: Monitorowanie i reagowanie na incydenty bezpieczeństwa
Zweryfikowanie zgodności z wymaganiami w zakresie zdefiniowania wymagań, wdrożenia i konfiguracji narzędzi, ciągłego monitorowania i skutecznego reagowania.

- 5) Obszar 5: Zarządzanie zmianą
Zweryfikowanie zgodności w wymaganiami w zakresie identyfikowania potrzeby zmian, ustalania wymagań bezpieczeństwa, wyboru rozwiązań, dokumentowania, testowania i wdrażania zmian.
- 6) Obszar 6: Zarządzanie ciągłością działania
Zweryfikowanie zgodności w wymaganiami w zakresie dokonania analizy i zdefiniowania wymagań dla ciągłości działania, wdrożenia rozwiązań zapasowych i redundantnych, testowaniu zdolności, przygotowania odpowiednich umów z dostawcami oraz nadzorowaniu ich sposobu zapewnienia ciągłości działania.
- 7) Obszar 7: Utrzymanie systemów informacyjnych
Zweryfikowanie zgodności w wymaganiami w zakresie ustalania i nadzorowania wymagań bieżącej eksploatacji systemów informacyjnych.
- 8) Obszar 8: Utrzymanie i rozwój systemów informacyjnych
Zweryfikowanie zgodności w wymaganiami w zakresie ustalania i nadzorowania wymagań bieżącej eksploatacji systemów informatycznych wykorzystywanych do zapewniania, monitorowania i reagowania na incydenty bezpieczeństwa.
- 9) Obszar 9: Bezpieczeństwo fizyczne
Zweryfikowanie zgodności w wymaganiami w zakresie skuteczności procesu ochrony fizycznej i środowiskowej.
- 10) Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług
Zweryfikowanie zgodności w wymaganiami w zakresie definiowania i nadzorowania stosowania wymagań bezpieczeństwa informacji i ciągłości działania przez dostawców usług bezpieczeństwa informacji oraz usług wdrażania i utrzymywania systemów informatycznych wykorzystywanych do świadczenia Usług Kluczowych.

III. Wymagania

1. Analiza musi zostać oparta na wymaganiach zawartych między innymi w:
 - 1) Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, 1222) wraz z aktami wykonawczymi do ww. ustawy;
 - 2) Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2022 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. 2024 poz. 773);
 - 3) Normie PN-EN ISO/IEC 27001;
 - 4) Normie PN-EN ISO 22301.
2. Zamawiający wymaga, aby Wykonawca wskazał w wykazie wykonanych usług w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, że wykonał, co najmniej 2 usługi wykonane na rzecz instytucji publicznych, obejmujące swoim zakresem wykonanie analizy w zakresie stanu systemu bezpieczeństwa wykorzystywanego do świadczenia usług kluczowej o wartości nie mniejszej niż 14 000 zł każda.
3. Zamawiający wymaga, aby analiza została przeprowadzona przez co najmniej 2 osoby, które posiadają przynajmniej jeden z poniższych certyfikatów:
 - 1) Certified Internal Auditor (CIA);

- 2) Certified Information System Auditor (CISA);
- 3) 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;
- 4) 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;
- 5) Certified Information Security Manager (CISM);
- 6) Certified in Risk and Information Systems Control (CRISC);
- 7) Certified Information Systems Security Professional (CISSP);
- 8) Systems Security Certified Practitioner (SSCP);
- 9) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.