Załącznik nr 1 do Zapytania

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest **wykonanie analizy stanu bezpieczeństwa systemu bezpieczeństwa wykorzystywanego do świadczenia usługi kluczowej.**

Zamawiający jest Operatorem Usługi kluczowej w obszarze:

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

I. Zakres prac.

- Analiza dokumentacji dotyczącą bezpieczeństwa IT;
- Analiza skuteczności funkcjonowania mechanizmów kontrolnych;
- Opracowanie raportu zawierającego opis zidentyfikowanych niezgodności oraz obserwacji wraz z rekomendacjami, w tym zalecanym harmonogramem I szacunkowym kosztem rekomendowanych zmian;
- Opracowanie streszczenia raportu;
- Przestawienie wyników analizy Kierownictwu organizacji (prezentacja na spotkaniu).

II. Obszary analizy.

- Obszar 1: Organizacja zarządzania bezpieczeństwem informacji

Zweryfikowanie zgodności z wymaganiami w zakresie stworzenia i utrzymywania systemu zarządzania zapewniającego zgodność z UKSC.

- 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.

- Obszar 3: Zarządzanie ryzykiem

Zweryfikowanie zgodności z wymaganiami w zakresie poprawności stosowanej metodyki zarządzania ryzykiem oraz kompletności procesu zarządzania ryzykiem poczynając od identyfikacji ryzyka aż po nadzór nad wprowadzeniem rekomendacji.

- 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 na potencjalne incydenty.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

- Obszar 5: Zarządzanie zmianą
  Zweryfikowanie zgodności w wymaganiami w zakresie identyfikowania potrzeby zmian, ustalania wymagań bezpieczeństwa, wyboru rozwiązań, dokumentowania, testowania i wdrażania zmian.

- 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.

- Obszar 7: Utrzymanie systemów informacyjnych

Zweryfikowanie zgodności w wymaganiami w zakresie ustalania i nadzorowania wymagań bieżącej eksploatacji systemów informacyjnych.

- 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.

- Obszar 9: Bezpieczeństwo fizyczne

Zweryfikowanie zgodności w wymaganiami w zakresie skuteczności procesu ochrony fizycznej i środowiskowej.

- 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:

   - Ustawie o krajowym systemie cyberbezpieczeństwa;
   - Aktach wykonawczych do ww. ustawy;
   - Rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności;
   - Normie PN-EN ISO/IEC 27001;
   - 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 usługi kluczowej o wartości nie mniejszej niż 20 000 zł każda.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3. Zamawiający wymaga, aby analiza została przeprowadzona przez co najmniej 2 osoby, które posiadają przynajmniej jeden z poniższych certyfikatów:

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);
- 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;
- 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;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706