237881

Załącznik nr 1

Opis Przedmiotu Zamówienia

Audyt w nadzorze Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami normy PN-ISO/IEC 27001 w Centrum e-Zdrowia

I **Przedmiot zamówienia:**

1. Przeprowadzenie audytu w nadzorze Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami normy PN-ISO/IEC 27001:2023-08 w Centrum e-Zdrowia, (zwanego dalej „Cez" lub Zamawiającym) stanowiącego potwierdzenie spełnienia przez organizację określonych wymagań bezpieczeństwa informacji i utrzymania ważności certyfikatu PN-ISO/IEC 27001.

II **Termin realizacji:**

1. **WARIANT I -** Przedmiot zamówienia będzie realizowany corocznie przez okres 3 kolejnych lat, z uwzględnieniem, że pierwszy audyt zostanie wykonany nie później niż do dnia 10 kwietnia 2026 r (zgodnie z aktualnie posiadanym przez Zamawiającego certyfikatem).
2. **WARIANT II -** Przedmiot zamówienia zostanie wykonany nie później niż do dnia 10 kwietnia 2026 r (zgodnie z aktualnie posiadanym przez Zamawiającego certyfikatem).
3. Audyt realizowany będzie w formie on-site lub on-line w dni robocze uzgodnione z Zamawiającym.

III **Zakres usługi**

Przeprowadzenie audytu w nadzorze ISO – przeglądu i diagnozy istniejącego systemu zarządzania w CeZ pod kątem spełnienia wymagań PN-ISO/IEC 27001, w tym analizy dokumentacji regulującej zasady funkcjonowania CeZ w celu utrzymania certyfikatu zgodności z ww. normą:

a. Opracowanie planu/harmonogramu audytu z Zamawiającym;
b. Przeprowadzenie audytu;
c. Przygotowanie i przekazanie Zamawiającemu w formie elektronicznej wstępnego raportu;
d. Przygotowanie i przekazanie Zamawiającemu w formie elektronicznej końcowego raportu;
e. W przypadku pozytywnego wyniku przeprowadzonego audytu, złożenie wniosku o wydanie certyfikatu na zgodność z normą PN-ISO/IEC 27001.

IV Produkty usługi

1. Harmonogram Audytu uzgodniony z Zamawiającym.
2. Wykonawca przedstawi wstępny (Zamawiający ma prawo wnieść zastrzeżenia i uwagi do wstępnego raportu) oraz końcowy raport z audytu, który będzie zawierał co najmniej:
   a. cel i zakres (obszaru) audytu,
   b. nazwa i opis stosowanej normy wg której zrealizowano audyt,
   c. opis metodyki audytu,
   d. imiona i nazwiska audytorów,
   e. opis przeprowadzonych prac,

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

f. ustalenia określone na podstawie materiału zgromadzonego w trakcie audytu,
g. ocenę stopnia spełniania wymagań,
h. sformułowane ewentualne niezgodności wraz z odniesieniem do normy,
i. rekomendacje wynikające z wymagań normy oraz ewentualnych działań korygujących z poprzedniego audytu.

3. Końcowy raport z audytu zostanie przekazane w terminie ustalonym z Zamawiającym.
4. Audytowa dokumentacja robocza, stanowiąca podstawę do sporządzenia raportu z audytu zostanie przekazana łącznie z częściowymi raportami, lecz nie będzie stanowiła załącznika do końcowego raportu z przeprowadzonego audytu.
5. W przypadku pozytywnej oceny zgodności z normą, zostanie wydany/utrzymany certyfikat Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001.
6. Warunki dostarczenia certyfikatu:
   a. Certyfikaty zostaną wydane w języku polskim i angielskim - po 1 szt. oraz w postaci elektronicznej,
   b. do 35 Dni Roboczych od dnia doręczenia Zamawiającemu końcowego raportu, w formie elektronicznej, z przeprowadzonego audytu.

V Wymagania odnośnie do jednostki audytującej i audytora

1. Podmiot audytujący musi posiadać akredytację w zakresie audytowania pomiotów informatycznych (Information Technology).
2. Audytor (audytorzy) przeprowadzający audyt w Centrum muszą mieć niezbędne uprawnienia do przeprowadzania Audytu w nadzorze normy PN-ISO/IEC 27001 w zakresie audytowania pomiotów informatycznych (Information Technology).
3. Audytor (audytorzy) powinien spełniać następujące wymagania:
   a. powinien legitymować się wykształceniem wyższym,
   b. co najmniej 1 audytor (w przypadku zespołu audytorów) powinien legitymować się co najmniej 2-letnim doświadczeniem[1] oraz przeprowadzeniem co najmniej 5 audytów zgodności Systemów Zarządzania Bezpieczeństwa Informacji z normą PN-ISO/IEC 27001 zrealizowanych w Nadzorze w jednostkach administracji publicznej.

VI Informacje ogólne o zatrudnieniu w CeZ objętym certyfikacją PN-ISO/IEC 27001

1. Na potrzeby szacowania prosimy przyjąć następujące założenie:
   a. ok 500 pracowników CeZ;
   b. ok 900 osób współpracujących.

[1] Przez „doświadczenie zawodowe w pracy, w jednostce administracji publicznej", Zamawiający rozumie dowolną formę zdobywania doświadczenia np. w drodze umowy o pracę, umowy zlecenia, umowy o dzieło, odbycia stażu – łącznie doświadczenia nie krótszego niż dwa lata.

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