

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 w Centrum e-Zdrowia, zwanego dalej „Centrum”, 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 w ciągu 6 dni roboczych, jednak nie później niż do dnia 10 kwietnia 2023 r (zgodnie z aktualnie posiadanym przez Zamawiającego certyfikatem).
- 2) **WARIANT II** - Przedmiot zamówienia zostanie wykonany w ciągu 6 dni roboczych, jednak nie później niż do dnia 10 kwietnia 2023 r (zgodnie z aktualnie posiadanym przez Zamawiającego certyfikatem).
- 3) Audyt realizowany będzie w formie on-line w dni robocze uzgodnione z Zamawiającym.

III. Zakres usługi

- 1) Przeprowadzenie audytu w nadzorze ISO - diagnozy istniejącego systemu zarządzania w Centrum pod kątem spełnienia wymagań PN-ISO/IEC 27001, w tym analizy dokumentacji regulującej zasady funkcjonowania Centrum w celu utrzymania certyfikatu zgodności z ww. normą.
- 2) Transfer certyfikacji oraz utrzymanie certyfikacji i rejestracji:
 - a) przegląd dokumentacji,
 - b) opracowanie planu audytu przeglądowego.
- 3) Przeprowadzenie audytu przeglądowego on-line, sprawdzającego użytkowanie certyfikacji.
- 4) Przegląd i ocena ewentualnych działań korygujących.
- 5) Opracowanie planu kolejnego audytu.
- 6) Przygotowanie raportu z audytu.

IV. Produkty usługi

- 1) Wykonawca przedstawi z audytu raport, który będzie zawierał co najmniej:
 - a) cel i zakres (obszaru) audytu,
 - b) stosowaną normę,
 - c) opis metodyki audytu,
 - d) imiona i nazwiska audytorów,
 - e) opis przeprowadzonych prac,
 - f) ustalenia (próbki) oraz dowody tych ustaleń,
 - g) ocenę spełniania wymagań,
 - h) sformułowane niezgodności wraz ze wskazaniem punktów normy, w których te niezgodności występują,
 - i) w przypadku zidentyfikowanych niezgodności, propozycję realizacji działań w badanym obszarze mających na celu spełnienie wymagań normy,
 - j) rekomendacje do działań korygujących.
- 2) Kompletny raport z audytu oraz propozycje działań mających na celu optymalizację/usprawnienie realizacji procesów w badanych obszarach – jeżeli zostaną zidentyfikowane podczas audytu, zostaną przekazane w terminie ustalonym z Zamawiającym. Zamawiający ma prawo wnieść zastrzeżenia

i uwagi do raportu.

- 3) 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.
- 4) W przypadku pozytywnej oceny zgodności z normą, zostanie wydany/utrzymany certyfikat Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001.
- 5) Certyfikaty zostaną wydane standardowo w języku polskim i angielskim - po 1 szt. oraz w postaci elektronicznej.

V. Wymagania odnośnie 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 doświadczeniem¹ oraz przeprowadzeniem co najmniej 5 audytów zgodności Systemów Zarządzania Bezpieczeństwem Informacji z normą PN-ISO/IEC 27001 zrealizowanych w Nadzorze w jednostkach administracji publicznej.

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.