Opis Przedmiotu Zamówienia

1. Przedmiotem zamówienia jest
2. Etap I i jedyny oznaczony jako – AUDYT 0 - usługa przeprowadzenia audytu (audyt **Ochrony Danych Osobowych , Wymagań Krajowych Ram Interoperacyjności** , **Wymagań Operatora Usługi Kluczowej** po decyzji o wyznaczeniu na Operatora Usług Kluczowych bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zwanego dalej "audytem" u operatora usługi kluczowej zgodnie z wymogami ustawy o krajowym systemie cyberbezpieczeństwa oraz aktów powiązanych pod kątem ich zgodności z przepisami oraz normami, o których mowa poniżej oraz przygotowanie i przekazanie Zamawiającemu pisemnego sprawozdania z przeprowadzonego audytu wraz z dokumentacją z przeprowadzonego audytu, zwanego dalej „raportem".

2. Na podstawie zebranych dokumentów i dowodów w ramach Etapu I audytorzy sporządzą pisemne sprawozdanie z przeprowadzonego audytu zgodne z szablonem sprawozdania z audytu zgodnego z ustawą KSC, opracowanym przez Ekspertów z ISSA Polska - Stowarzyszenia do spraw Bezpieczeństwa Systemów Informacyjnych oraz IIA Polska - Instytutu Audytorów Wewnętrznych pod nadzorem ówczesnego Ministerstwa Cyfryzacji (https://www.gov.pl/web/baza-wiedzy/szablony-audytudla-operatorow-uslug-kluczowych
3. Celem audytu jest potwierdzenie zgodności bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia Usług Kluczowych z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa.

Ocena bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług kluczowych realizowanych przez Szpital oraz identyfikacja i analiza luki zgodności z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa przeprowadzona powinna zostać w oparciu o 10 obszarów tj.:

- Obszar 1: Organizacja zarządzania bezpieczeństwem informacji
- Obszar 2: Procesy zarządzania bezpieczeństwem informacji
- Obszar 3: Zarządzanie ryzykiem
- Obszar 4: Monitorowanie i reagowanie na incydenty bezpieczeństwa
- Obszar 5: Zarządzanie zmianą
- Obszar 6: Zarządzanie ciągłością działania
- Obszar 7: Utrzymanie systemów informacyjnych
- Obszar 8: Utrzymanie i rozwój systemów informacyjnych
- Obszar 9: Bezpieczeństwo fizyczne
- Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług

Szczegółowy opis przedmiotu zamówienia

1. Przeprowadzenie audytu w zakresie sprawdzenia dostosowania Zamawiającego jako operatora usługi kluczowej do wymogów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (zwana dalej Ustawą), wraz z powiązanymi aktami wykonawczymi, w zakresie wymagań, jakie operatorzy usług kluczowych zobowiązani są spełnić na podstawie decyzji o uznaniu za operatora usługi kluczowej, a w tym:

a. wykonanie audytu zerowego bezpieczeństwa, w tym

- inwentaryzacji obszarów z przetwarzaniem informacji w systemach informacyjnych wraz z otoczeniem,
- identyfikacja informacji i jej klasyfikacja,
- inwentaryzacja zasobów infrastruktury teleinformatycznej, oprogramowania i obszarów bezpiecznych,
- identyfikacja podatności,
- identyfikacja dostawców,
- inwentaryzacja procedur,
- przegląd dokumentacji,
- zidentyfikowaniu wszelkich niezgodności i wdrożenie działań naprawczych,

b. przeprowadzenie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej zgodnego z wymogami ustawy KSC w szczególności zgodnie z zapisem art. 15 ust. 2 pkt 2 lit a ustawy KSC, w tym:

- Weryfikacja przywództwa
- Weryfikacja polityk bezpieczeństwa
- Weryfikacja ról, odpowiedzialności i uprawnień
- Weryfikacja działań odnoszących się do ryzyka i szans
- Weryfikacja wsparcia dla SZBI, w tym zasoby, kompetencje, uświadamianie, komunikację i dokumentowanie
- Weryfikacja działań operacyjnych i ciągłości działania
- Weryfikacja adekwatności zabezpieczeń do zidentyfikowanych zagrożeń,
- Weryfikacja oceny wyników SZBI w tym monitorowanie, pomiary, analiza, ocena, audyty wewnętrzne i przeglądy zarządzania
- Weryfikacja ciągłego doskonalenia
- Weryfikacja zgodności dokumentacji z normami i stanem faktycznym

<u>Wymagania dotyczące Wykonawcy</u>

1. W postępowaniu może wziąć udział Wykonawca, który dysponuje zespołem spełniającym wymagania ustawy o krajowym systemie cyberbezpieczeństwa. Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia

wykazane w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r. poz. 1369 z późn. zm.).

2. Wykonawca musi posiadać doświadczenie w przeprowadzaniu co najmniej 2 usług audytorskich na kwotę nie mniejsza niż 20.000,00 zł odpowiadających swoim rodzajem usłudze stanowiącej przedmiot zamówienia w przeciągu 4 lat od terminu składania ofert
3. Dodatkowo celem zapewnienia bezpieczeństwa informacji przekazywanych w ramach realizacji przedmiotu zamówienia Wykonawca musi posiadać aktualny certyfikat zgodności z wymaganiami normy ISO27001, wydany przez jednostkę oceniającą zgodność, akredytowaną przez Polskie Centrum Akredytacji.
4. W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia ~~wraz z formularzem oferty~~ wykazu osób przewidzianych do realizacji zamówienia, kopii certyfikatów oraz wykazu zrealizowanych usług audytorskich.
5. Audytorzy zobowiązani są do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzonym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.
6. Podstawowe informacje dotyczące Szpitala Wojewódzkiego w Poznaniu – w związku z koniecznością zabezpieczenia teleinformatycznego Szpitala szczegółowe informacje zostaną podane na etapie realizacji zadania.

- Liczba lokalizacji: 3
- Ogólna liczba pracowników: 1800
- Liczba pracowników IT: 6 osób
- Ilość systemów wykorzystywanych do świadczenia usługi kluczowej: 6
- Liczba stanowisk komputerowych: >500

Oczekiwany produkt finalny.

Zamawiający wymaga, aby produkt finalny stanowiła ocena systemu bezpieczeństwa cybernetycznego Zamawiającego zgodnie z Ustawą, obejmująca:

ETAP I:

Opracowanie raportu przeprowadzonej analizy zgodnie z metodyką wymaganą w ustawie o KSC, zawierającego:

- określenie niezgodności,

- dla zgodności określenie potencjału do doskonalenia i opracowanie rekomendacji dotyczących wdrożenia wymaganych ustawą zabezpieczeń organizacyjnych i technicznych
- Wytyczne, rekomendacje oraz opisy techniczne rozwiązań (wraz z szacunkową wyceną) dotyczące sposobu wdrożenia odpowiednich, do oszacowanego ryzyka, środków technicznych i organizacyjnych