Załącznik NR 2

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

Przedmiot zamówienia:

Audyt końcowy cyberbezpieczeństwa dla SZPZOZ im. Dzieci Warszawy w Dziekanowie Leśnym w ramach projektu: „Przyspieszenie procesów transformacji cyfrowej w SZPZOZ im. Dzieci Warszawy w Dziekanowie Leśnym" Nabór: KPOD.07.03-IP.10-001/25, Numer wniosku: KPOD.07.03-IP.10-0332/25.

1. Wymagania ogólne dotyczące audytu końcowego cyberbezpieczeństwa

1.1. Zamówienie realizowane jest w ramach Krajowego Planu Odbudowy i Zwiększania Odporności i musi być zgodne z zasadą „Do No Significant Harm" (DNSH), o której mowa w art. 17 Rozporządzenia (UE) 2020/852,

1.1.1. Przedmiot zamówienia obejmuje wyłącznie audyt z zakresu cyberbezpieczeństwa, ma charakter niematerialny i nie powoduje znaczących szkód środowiskowych w żadnym z celów środowiskowych określonych w ww. rozporządzeniu,

1.1.2. Na żądanie Zamawiającego Wykonawca złoży oświadczenie o zgodności realizacji zamówienia z zasadą DNSH.

1.2. Gdziekolwiek w opisie przedmiotu zamówienia przywołane są normy lub nazwy własne lub znaki towarowe lub patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę Zamawiający dopuszcza rozwiązania równoważne.

1.2.1. Certyfikaty i normy wskazane przez Zamawiającego jako wymagane mogą być zastąpione certyfikatami i normami równoważnymi,

1.2.2. Wykonawca jest zobowiązany wykazać, że certyfikat równoważny potwierdza posiadanie co najmniej takiej samej wiedzy, kompetencji, doświadczenia co certyfikat wskazany przez Zamawiającego. Jako certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu wskazanego certyfikatu, wydany przez niezależną jednostkę certyfikującą posiadającą akredytację uznawaną w krajach Unii Europejskiej, co jest rozumiane jako:

1.2.2.1. analogiczna dziedzina merytoryczna wynikająca z wiedzy, której dotyczy certyfikat,

1.2.2.2. analogiczny stopień poziomu kompetencji,

1.2.2.3. analogiczny poziom doświadczenia zawodowego wymagany dla otrzymania danego certyfikatu (np.: konieczność wykazania się uczestnictwem w określonej liczbie projektów w danej roli, etc.),

1.2.2.4. uzyskanie certyfikatu potwierdzone egzaminem, o ile był wymagany,

1.2.2.5. został wydany przez podmiot profesjonalnie zajmujący się certyfikowaniem, nie powiązany z Wykonawcą, posiadający uprawnienia do wydawania certyfikatów nadane przez niezależną od Wykonawcy jednostkę (certyfikat równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy),

1.2.3. Jako normę równoważną np. normie ISO/IEC Zamawiający dopuszcza inne międzynarodowe normy standaryzujące analogiczne do dziedziny merytorycznej objętej wskazaną normą.

1.3. Wszystkie poniższe parametry należy traktować jako minimalne.

1.4. Wykonawca nie może żądać dodatkowego wynagrodzenia, jeśli dostarczone elementy służące do realizacji przedmiotu zamówienia posiadać będą większą funkcjonalność niż wymagana niniejszym OPZ.

1.5. Wszelkie użyte nazwy własne producentów należy traktować jedynie informacyjnie, Zamawiający dopuszcza możliwość zastosowania technologii równoważnej zapewniającej poniższe funkcjonalności.

1.6. Wykonawca powinien zgłosić gotowość do realizacji przedmiotu zamówienia do 10 dni od dnia podpisania umowy.

1.7. Wykonawca zobowiązuje się do zgłaszania Zamawiającemu niezwłocznie uwag w postaci pisemnej notatki w przypadku stwierdzenia niezgodności którejkolwiek z zastosowanych/wdrożonych funkcjonalności przez Zamawiającego w ramach projektu „Przyspieszenie procesów transformacji cyfrowej w SZPZOZ im. Dzieci Warszawy w Dziekanowie Leśnym" realizowanego w ramach KPO z planowanym celem, jakim jest potwierdzenie skuteczności wdrożonych rozwiązań oraz zgodności środowiska IT z wymaganiami KPO. Po wykonaniu odpowiednich poprawek przez innych Wykonawców realizujących zadania w ramach w/w projektu audytor ponownie zweryfikuje wspomniane niezgodności umożliwiając przy tym potwierdzenie skuteczności wdrożonych rozwiązań.

1.8. Wykonawca przygotuje i przekaże Zamawiającemu audyt końcowy zgonie z opisem zawartym w pkt 2 – Realizacja audytu cyberbezpieczeństwa".

2. Realizacja audytu cyberbezpieczeństwa

Prawidłową realizacją przedmiotu zamówienia jest przeprowadzenie audytu cyberbezpieczeństwa, którego celem jest potwierdzenie skuteczności wdrożonych rozwiązań oraz zgodności środowiska IT z wymaganiami KPO.

1. Audyt końcowy ma na celu potwierdzenie zgodności wdrożonej infrastruktury technicznej Szpitala z wymaganiami projektu KPO D1.1.2, w szczególności wskaźnika D21G.R2. Celem audytu jest ocena poziomu dojrzałości w obszarze cyberbezpieczeństwa oraz skuteczności wdrożonych polityk, procedur i zabezpieczeń organizacyjno-technicznych. Wynik audytu musi zawierać komplet materiałów niezbędnych do prawidłowego rozliczenia przedsięwzięcia.

2. Audyt obejmuje wszystkie obszary, w których przetwarzane są dane osobowe i dane medyczne, w tym kluczowe systemy informacji medycznej (HIS, LIS, RIS/PACS, EDM), infrastrukturę urządzeń medycznych, systemy administracyjne, sieć komputerową, serwery, stacje robocze oraz systemy kopii zapasowych. Audyt ma potwierdzić zgodność z wymaganiami PN-EN ISO/IEC 27001:2022, Rozporządzenia KRI, ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz RODO.

3. Audyt powinien obejmować ocenę zarówno organizacyjną, jak i techniczną, w tym:

a. strukturę organizacyjną bezpieczeństwa informacji, role i odpowiedzialności,

b. proces zarządzania ryzykiem i incydentami bezpieczeństwa,

c. ciągłość działania i ochronę danych (BIA, kopie zapasowe),

d. bezpieczeństwo sieci i urządzeń brzegowych (firewall, segmentacja sieci),

e. bezpieczeństwo serwerów, platform wirtualizacyjnych i stacji roboczych,

f. kontrolę dostępu, uwierzytelnianie użytkowników i zarządzanie uprawnieniami,

g. logowanie zdarzeń i analizę bezpieczeństwa systemów,

h. zarządzanie aktualizacjami i łatami bezpieczeństwa,

i. mechanizmy kopii bezpieczeństwa i przywracania danych.

4. Audyt zostanie przeprowadzony zgodnie z zasadami PN-EN ISO/IEC 19011:2018 i oparty na metodyce audytowej stosowanej w systemach zarządzania bezpieczeństwem informacji. Obejmie przegląd dokumentacji SZBI, wywiady z personelem, analizę konfiguracji technicznej oraz testy kontrolne wybranych mechanizmów zabezpieczeń. Audyt końcowy może być realizowany w trybie mieszanym (zdalnym i stacjonarnym).

5. Wyniki audytu zostaną przedstawione w formie raportu zawierającego: opis stanu faktycznego, listę niezgodności i obserwacji, ocenę poziomu dojrzałości cyberbezpieczeństwa, rekomendacje działań doskonalących oraz wypełnioną ankietę dojrzałości zgodnie z wymaganiami projektu KPO D1.1.2. Raport musi być podpisany przez audytora wiodącego.

6. Zespół audytujący musi składać się z co najmniej dwóch audytorów posiadających certyfikaty określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Co najmniej jeden z Audytorów musi posiadać poniższe certyfikaty:

a. 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,

b. 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,

lub

co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub jednostka oceniająca zgodność,

akredytowana zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 z późn.zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych. Osoby wykonujące czynności audytowe nie mogą pozostawać w jakiejkolwiek relacji, która mogłaby wpływać na ich obiektywizm, bezstronność lub niezależność zawodową. W szczególności audytor nie może być powiązany z jednostką audytowaną poprzez zależność służbową, finansową, osobistą ani organizacyjną.

7. W ramach Audytu należy opracować również ankietę weryfikacji dojrzałości pod kątem cyberbezpieczeństwa zgodnie z regulaminem projektu „Przyspieszenie procesów transformacji cyfrowej w SZPZOZ im. Dzieci Warszawy w Dziekanowie Leśnym" Nabór: KPOD.07.03-IP.10-001/25, Numer wniosku: KPOD.07.03-IP.10-0332/25.