Załącznik nr 3c do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

PAKIET NR 3 – Audyt poziomu bezpieczeństwa teleinformatycznego

Przedmiotem zamówienia jest audyt wykonany na potrzeby i na podstawie „ZARZĄDZENIE NR 117/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 września 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców" .

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z przedmiotowym zarządzeniem oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie „Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa". Przeprowadzony audyt powinien wykazać podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, czy spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa w placówce.

I. Zamawiający Informuje, że audytem objęte będzie środowisko składające się z :

1) liczba stacji roboczych (komputerów) – 135
2) liczba urządzeń mobilnych (laptopy) – 7
3) liczba urządzeń mobilnych (tablety) – 11
4) liczba serwerów fizycznych – 9
5) liczba serwerów wirtualnych – 16
7) liczba pracowników korzystających z urządzeń informatycznych – 225

II. Termin realizacji:
Przedmiot zamówienia musi zostać wykonany do dnia **30 listopada 2022 roku.** z zastrzeżeniem, że Raport z audytu końcowego poziomu bezpieczeństwa teleinformatycznego u Zamawiającego i przekazanie go Zamawiającemu nastąpi w terminie nie dłuższym niż do **9 grudnia 2022 r.**

Ramowy harmonogram wykonania usługi:

1) Spotkanie koordynacyjne Stron i szczegółowe zaplanowanie realizacji usługi - do 7 dni roboczych od dnia zawarcia Umowy,
2) Audyt początkowy – audyt mający na celu zapoznanie się ze stanem początkowym dot. poziomu bezpieczeństwa teleinformatycznego w placówce opierający się na ocenie ankietowej placówki wynikającą z zarządzenia.
3) Przeprowadzenie końcowego Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego po wdrożeniu przez Zamawiającego czynności podnoszących poziom bezpieczeństwa systemów teleinformatycznych - do 7 dni roboczych od dnia powiadomienia przez Zamawiającego Wykonawcy o gotowości do poddania się Audytowi.

Powiadomienie Wykonawcy przez Zamawiającego o gotowości do poddania się Audytowi powinno nastąpić nie później niż do dnia 30 listopada 2022r

4) Sporządzenie Raportu z Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego i przekazanie go Zamawiającemu - do 7 dni roboczych od dnia zakończenia Audytu.

III. Audyt bezpieczeństwa może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2) co najmniej dwóch audytorów posiadających:
a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność;
4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność;
5) Certified Information Security Manager (CISM);
6) Certified in Risk and Information Systems Control (CRISC);
7) Certified in the Governance of Enterprise IT (CGEIT);
8) Certified Information Systems Security Professional (CISSP);
9) Systems Security Certified Practitioner (SSCP);
10) Certified Reliability Professional;
11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

IV. Obszary Audytu:

Audyt poziomu bezpieczeństwa teleinformatycznego w placówce powinien uwzględniać elementy wdrożone w ramach realizacji aspektów wskazanych przez Zamawiającego podczas realizacji umowy z NFZ w ramach rzeczonego zarządzenia. Wyniki audytu muszą zostać oparte na rekomendacji dot. zasadności i kompletności realizacji projektu.

a) Ocena skuteczności działania infrastruktury:

- urządzenia i konfiguracja w zakresie ochrony poczty,
- urządzenia i konfiguracja w zakresie ochrony sieci,
- urządzenia i konfiguracja w zakresie systemów serwerowych,
- urządzenia i konfiguracja w zakresie stacji roboczych,
- urządzenia i konfiguracja w zakresie systemów bezpieczeństwa.

b) Zarządzanie bezpieczeństwem informacji:

- nośniki wymienne - udokumentowany sposób postępowania,
- zarządzanie tożsamością / dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu,

c) Monitorowanie i reagowanie na incydenty bezpieczeństwa:

- procedury zarządzania incydentami,
- raportowanie poziomów pokrycia scenariuszami znanych incydentów,
- dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa,
- monitorowanie i wykrycie incydentów bezpieczeństwa,
- Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.

d) Zarządzanie ciągłością działania:

- konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa,
- raport z przeglądów i testów odtwarzania kopii bezpieczeństwa,
- procedury wykonywania i przechowywania kopii zapasowych,
- strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP),
- procedury utrzymaniowe.

e) Utrzymanie systemów informacyjnych:

- harmonogramy skanowania podatności,
- aktualny status realizacji postępowania z podatnościami,
- procedury związane ze z identyfikowaniem (wykryciem) podatności,

f) Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:

- polityka bezpieczeństwa w relacjach z dostawcami,
- standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa,
- dostęp zdalny,
- metody uwierzytelnienia.

V. Kryteria Audytu Bezpieczeństwa oparte są o:

a) Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa.
b) Wymagania normatywne PN-EN ISO/IEC 27001:2017-06.
c) Wewnętrzną dokumentację świadczeniodawcy.
d) Przepisy o Krajowym Systemie Cyberbezpieczeństwa.
e) Standardy Krajowych Ram Interoperacyjności (KRI).

VI. Wymagania dodatkowe Zamawiającego:

1. Wykonawca musi udokumentować doświadczenie w realizacji projektów informatycznych dla placówek ochrony zdrowia.
2. Część usługi „Audyt początkowy" powinna być wykonana nie później niż 7 dni od momentu podpisania umowy.
3. Cześć usługi „Opracowanie wyników po realizacji projektu" powinna być wykonana w ciągu 2 tyg. od momentu przedstawienia przez Zamawiającego informacji o realizacji wszystkich wydatków związanych z ZARZĄDZENIEM NR 117/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 września 2022 r.