Załącznik nr 1 do Zapytania ofertowego

I. Opis Przedmiotu Zamówienia

1. Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego (dalej jako „Audyt") oraz sporządzenie raportu z audytu z wynikami wykonanych czynności (zwanego dalej: „Raportem"), którego szczegółowy zakres określa Załącznik nr 1 do Opisu Przedmiotu Zamówienia (dalej OPZ).

2. Celem audytu jest dokonanie oceny poziomu bezpieczeństwa teleinformatycznego Zamawiającego po zrealizowaniu czynności, które mogą zostać objęte finansowaniem zgodnie z **ZARZĄDZENIEM NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców** - (**załącznik nr 2 do OPZ),** w odniesieniu do stanu bezpieczeństwa teleinformatycznego Zamawiającego istniejącego na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Zamawiającego w formie „Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa" (**załącznik nr 3 do OPZ**).

3. Z Przeprowadzonego Audytu Wykonawca sporządzi Raport , z którego będzie wynikać podniesienie poziomu bezpieczeństwa teleinformatycznego Zamawiającego w odniesieniu do poziomu wynikającego z „Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa" lub jego brak.

4. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

5. **Zakres audytu** obejmował będzie czynności, które, mogą zostać objęte finansowaniem w przypadku wykazania przez Zamawiającego, wynikiem audytu bezpieczeństwa, zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej. Do czynności tych należą:

1) zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa, w szczególności:

a) systemów kopii bezpieczeństwa, odmiejscowienia kopii, segmentacji w celu odseparowania urządzeń backupu, zapewnienia mechanizmów weryfikacji poprawności i odtwarzalności kopii i backupu,

b) systemów kontroli dostępu administracyjnego, zarządzania uprawnieniami (IAM/IDM),

c) urządzeń i oprogramowania typu firewall - zapora sieciowa z wbudowanym IPS oraz systemem antywirusowym oraz platform niezbędnych do ich uruchomienia,

d) systemów zapewniających bezpieczny system poczty elektronicznej, włączając w to systemy weryfikacji załączników i treści korespondencji oraz systemy wieloskładnikowego uwierzytelniania,

e) rozwiązań zapewniających ochronę DNS (DNS Protection) z użyciem systemów lokalnych (licencja oraz wsparcie w okresie do dnia 31 grudnia 2022 r.),

f) systemu typu SIEM,

g) systemu typu NAC – jako system lokalny;

2) zakup usługi wdrożenia i konfiguracji urządzeń i oprogramowania, o których mowa w pkt 1, oraz wsparcia eksperckiego w zakresie cyberbezpieczeństwa przez okres do dnia 31 grudnia 2022 r.;

3) zakup i wdrożenie systemu (usługi) typu SOC – przez okres do dnia 31 grudnia 2022 r.;

4) zakup usługi skanów podatności, w zakresie sprecyzowanym w materiale referencyjnym „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia”, opublikowanym na stronie internetowej Centrum e-Zdrowia), przez okres do dnia 31 grudnia 2022 r.;

5) zakup opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655) - jeśli dotyczy świadczeniodawcy będącego operatorem usługi kluczowej, o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii;

6) zakup szkolenia lub szkoleń w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych u świadczeniodawcy w zakresie podstawowej świadomości bezpieczeństwa IT, w tym:

a) ochrony przed zaawansowanymi atakami przez pocztę i WWW,

b) tworzenia i zarządzania polityką haseł i tożsamości,

c) zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),

d) wykonywania kopii zapasowych oraz tworzenia i utrzymania polityki ciągłości działania.

II. Ramowy harmonogram wykonania usługi:

1. Spotkanie koordynacyjne i szczegółowe planowanie realizacji usługi: do 7 dni roboczych od dnia zawarcia Umowy,
2. Wnikliwa analiza poziomu bezpieczeństwa teleinformatycznego Zamawiającego ze stanu początkowego z uwzględnieniem Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa. Głównym aspektem analizy powinny być elementy możliwe do finansowania opisane w pkt. 5 OPZ (odpowiednio Rozdziale 2 Zarządzenia prezesa NFZ) - do 14 dni roboczych od dnia zawarcia Umowy,
3. Przeprowadzenie 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 15 listopada 2022 r.**
4. Sporządzenie pisemnego Raportu z Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego i doręczenie go Zamawiającemu - do 7 dni roboczych od dnia zakończenia Audytu.

III. Dodatkowe wymagania:

1 Audyt poziomu bezpieczeństwa, o którym mowa w OPZ 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.

2. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1). Certified Internal Auditor (CIA); 1) Certified Information System Auditor (CISA);

2) 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,* w zakresie certyfikacji osób;

3) 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;

4) Certified Information Security Manager (CISM);

5) Certified in Risk and Information Systems Control (CRISC);

6) Certified in the Governance of Enterprise IT (CGEIT);

7) Certified Information Systems Security Professional (CISSP);

8) Systems Security Certified Practitioner (SSCP);

9) Certified Reliability Professional;

10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

IV. Załączniki:

1. Załącznik nr 1 - Zakres Raportu
2. Załącznik nr 2 ZARZĄDZENIE NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców
3. Załącznik nr 3 - Ankieta weryfikacji dojrzałości pod kątem bezpieczeństwa