Przedmiot zamówienia

1. Przedmiotem niniejszego zamówienia jest wykonanie audytu cyberbezpieczeństwa dla Powiatowego Centrum Zdrowia w Kamiennej Górze Sp. z o.o.
2. Przedmiot zamówienia obejmuje następujący zakres usług:
   a) wykonanie audytu cyberbezpieczeństwa w ramach umowy z NFZ w kontekście Zarządzenia 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 oraz Planu działania w zakresie cyberbezpieczeństwa w ochronie zdrowia,
   b) szkolenie kadry zarządzającej oraz osób zatrudnionych u Zamawiającego w zakresie podstawowej świadomości bezpieczeństwa IT.
3. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowej diagnozy bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu (w tym w szczególności weryfikacji struktury organizacji, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy poczty email, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli u Zamawiającego) oraz opracowania dokumentacji - raportu z wytycznymi do doskonalenia i rekomendacjami.
4. Audyt cyberbezpieczeństwa musi zostać przeprowadzony zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 r. poz. 1369 z późn. zm.) oraz Rozporządzeniem 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. 2017 poz. 2247), zwane dalej Rozporządzeniem KRI.
5. Audyt musi zostać wykonany zgodnie z formularzem zamieszczonym w dokumentacji Zarządzenia NR 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022r. - Opis działań skutkujących podniesieniu poziomem bezpieczeństwa teleinformatycznego u świadczeniodawcy - załącznik nr 2 do umowy z NFZ.
6. **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 audyt, **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.
7. **Audyt cyberbezpieczeństwa musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn. zm.).**
   Wykaz certyfikatów wskazanych w w/w rozporządzeniu:
   a) Certified Internal Auditor (CIA)
   b) Certified Information System Auditor (CISA)
   c) 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.

d) 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 (t.j. Dz.U. z 2022 r. poz. 5), w zakresie certyfikacji osób.
e) Certified Information Security Manager (CISM)
f) Certified in Risk and Information Systems Control (CRISC)
g) Certified in the Governance of Enterprise IT (CGEIT)
h) Certified Information Systems Security Professional (CISSP)
i) Systems Security Certified Practitioner (SSCP)
j) CertifiedReliability Professional
k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 CybersecurityExpert

8. Szkolenie w zakresie cyberbezpieczeństwa dla kadry zarządzającej Zamawiającego (stacjonarne) oraz osób zatrudnionych u Zamawiającego w zakresie podstawowej świadomości bezpieczeństwa IT (on-line) zakończone wydaniem certyfikatów, w tym:
   a) ochrony przed zaawansowanymi atakami przez pocztę i stronę 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.

9. Zakres obowiązków Wykonawcy:
   a) Wykonawca zobowiązany jest do kompleksowej realizacji zamówienia, tj. wykonania audytu cyberbezpieczeństwa, przeprowadzenia szkolenia w zakresie podstawowej świadomości bezpieczeństwa IT wypełnienia i podpisania wymaganych dokumentów 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 oraz ich dostarczenia w wersji elektronicznej i papierowej do siedziby Zamawiającego (po jednym egzemplarzu).
   b) W ramach zamówienia Wykonawca zobowiązany jest do przeprowadzenia audytu cyberbezpieczeństwa w siedzibie Zamawiającego. Zamawiający nie dopuszcza możliwości realizacji zamówienia za pomocą środków zdalnej komunikacji.
   c) Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym koszty ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku i skanu dokumentów.
   d) Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji na każdym etapie realizacji zamówienia, aż do zaakceptowania dokumentów przez Zamawiającego.