Oznaczenie sprawy: 08/2022 Załącznik Nr 2 do Zaproszenia

**OPIS PRZEDMIOTU ZAMÓWIENIA**

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, lub

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu (min. jeden certyfikat z wykazu dla każdego z audytorów),

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);

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.

**Audyt bezpieczeństwa systemów IT**

Przedmiotem zamówienia jest Przeprowadzenie audytu bezpieczeństwa, którego celem jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa i oceny podniesienia poziomu bezpieczeństwa teleinformatycznego, 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.

Obszary Audytu (raportu):

1. Ocena skuteczności działania infrastruktury w zakresie urządzeń i konfiguracji w zakresie: ochrony poczty, ochrony sieci, systemów serwerowych, stacji roboczych, systemów bezpieczeństwa,
2. Zarządzanie bezpieczeństwem informacji:
   * nośniki wymienne - udokumentowany sposób postępowania,
   * zarządzanie tożsamością/dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu,
3. 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.
4. 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.
5. Utrzymanie systemów informacyjnych:
   * harmonogramy skanowania podatności,
   * aktualny status realizacji postępowania z podatnościami,
   * procedury związane ze z identyfikowaniem (wykryciem) podatności,
   * współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.
6. 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.

Kryteria Audytu Bezpieczeństwa oparte będą o:

1. Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa.
2. Wymagania normatywne PN-EN ISO/IEC 27001:2017-06.
3. Wymagania normatywne PN-EN ISO 22301:2020-04.
4. Wewnętrzną dokumentację Zamawiającego.
5. Przepisy o Krajowym Systemie Cyberbezpieczeństwa.
6. Standardy Krajowych Ram Interoperacyjności (KRI).
7. Zakresem Audytu objęta będzie cała działalność świadczeniodawcy.

Wymagania dla jednostki przeprowadzającej audyt:

Zamawiający wymaga, aby jednostka przeprowadzająca audyt spełniała wymagania określone w:

* Załączniku nr 2 do 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

* Ustawie z dnia 5 lipca 2018r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560).