**Załącznik nr 2 – Opis przedmiotu zamówienia**

**Piekary 30.08.2022**

**„Przeprowadzenie 1 etapowego audytu bezpieczeństwa systemu informacyjnego i ochrony danych medycznych dla zgodnie z wymaganiami Zarządzenia nr 8/2023/BBIICD prezesa Narodowego Funduszu Zdrowia w SP Wojewódzkim Szpitalu Chirurgii Urazowej im. dr. Janusza Daaba w Piekarach Śląskich”**

Zakres audytu

Ocena stopnia dojrzałości i zgodności organizacyjno - technicznej infrastruktury ICT w kontekście zabezpieczeń konfiguracji, eksploatacji modernizacji ICT Zamawiającego.

Wymagania dotyczące audytu bezpieczeństwa

1. 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.

2. 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, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

4) 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;

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.

3. Celem audytu jest wykazanie przez Świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności zgodnie z niniejszym zarządzeniem oraz w obszarach wskazanych w poniższej tabeli w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak.

|  |  |
| --- | --- |
| **Nazwa obszaru** | **Opis działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u Świadczeniodawców** |
| Skuteczność 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. |
| Procesy zarządzania bezpieczeństwem informacji. | -Nośniki wymienne - udokumentowany sposób postępowania.  -Zarządzanie tożsamością/dostęp do systemów w zakresie:  - - przydzielanie dostępu,  - - odbieranie dostępu.  -Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa. |
| 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. |
| 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. |
| 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. |
| 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. |
| Weryfikacja podniesienia poziomu bezpieczeństwa. | Przeprowadzony audyt wykazał podniesienie poziomu bezpieczeństwa teleinformatycznego w stosunku do stanu sprzed przystąpienia do działań mających na celu podniesienie poziomu bezpieczeństwa teleinformatycznego finansowanych w ramach zarządzenia. |

Wynikiem audytu będzie raport zawierający co najmniej:

* Opisy zidentyfikowanych nieprawidłowości wraz ze wskazaniem miejsc ich występowania,
* Wskazania zebranych dowodów audytowych,
* Rekomendacje wskazujące sposoby eliminacji zidentyfikowanych nieprawidłowości
* Wypełniony formularz samooceny dojrzałości organizacji zgodny z wzorem stosowanym przez NFZ
* Podsumowanie dla kierownictwa przedstawiające w sposób syntetyczny wnioski, oceny i rekomendacje audytowe

Czas realizacji zamówienia: zakończenie audytu i przedstawienie wniosków do 26 września 2023