# Opis Przedmiotu Zamówienia Audyt cyberbezpieczeństwa systemu informatycznego Szpitala Klinicznego im. dr. Józefa Babińskiego w Krakowie

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z zarządzeniem NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa

## Zakres audytu:

1. Skuteczność działania infrastruktury:
	1. w systemie poczty elektronicznej
	2. w zakresie konfiguracji i ochrony sieci
	3. w zakresie tworzenie kopi zapasowych i kopi bezpieczeństwa
	4. w zakresie zabezpieczenia stacji roboczych działających w zasobach Szpitala

## Raport z audytu:

1. Raport podsumowujący wydany przez audytora wiodącego w formie drukowanej oraz w wersji elektronicznej.
2. Minimalny zakres informacji w tekście audytu:
	1. Interpretacje zespołu audytorskiego wymagań określonych w ustawie o Krajowym Systemie Cyberbezpieczeństwa ze szczególnym odniesieniem się do niezbędnego zakresu stosowania wymagań formalnych bezpieczeństwa i ciągłości działania w organizacji i procesów kluczowych z wykluczeniem procesów merytorycznych
	2. rekomendacje dla organizacji w zakresie wymagań polityk bezpieczeństwa informacji i audytu wymaganego ustawą.
	3. rekomendacje działań korygujących lub naprawczych w systemie dokumentacyjnym w aktualnym polityk bezpieczeństwa informacji
	4. rekomendacje działań korygujących lub naprawczych w systemie dokumentacyjnym w kontekście wymagań polityki ciągłości działania
	5. jeżeli wymagane, rekomendacje w zakresie infrastruktury sieciowej: jej architektury, konfiguracji, stosowanych zabezpieczeń, adekwatności do wymaganego/oczekiwanego poziomu bezpieczeństwa
	6. jeżeli wystąpią: rekomendacje w zakresie poprawy technologii oraz jakości wykonania dla infrastruktury sieciowej.
	7. porównanie stanu badanych pól działalności Szpitala opisanych w ankiecie ze stanem obecnym.
3. Dokumentacja powykonawcza (w zakresie uzgodnionym z Zamawiającym( w 3 egzemplarzach w wersji papierowej oraz elektronicznej (płyta CD/DVD) w ustalonym między stronami formacie (Zakres raportu w wersji edytowanej docx. Zestawienie tabelarycznej w postaci edytowalnego MS Excel, rysunki, schematy w postaci pdf)

## Kryteria oceny systemu:

* 1. normy IEC 62443
	2. norma PN ISO/IEC 27001
	3. norma PN ISO/IEC 22301
	4. norma PN ISO/IEC 20000
	5. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2018 r. poz. 1560, z 2019 r. poz. 2020)
	6. Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018 r., poz. 2080)
	7. Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1780

## Harmonogram realizacji:

* 1. prace obiektowe: przewidywane do 5 dni (możliwe prace w dni weekendowe lub ustawowo wolne od pracy); harmonogram i sposób realizacji będzie dostosowywany do uwarunkowań ruchowych
	2. wykonanie raportu wersja robocza : do 7 dni licząc od daty otrzymania zamówienia
	3. weryfikacja po stronie Zamawiającego: do 2 dni o otrzymania raportu wersji roboczej
	4. wykonanie raportu w wersji finalnej: do 2 dni od opinii Zamawiającego

## Ogólne warunki realizacji.

Przeprowadzenie audytu w pełnym zakresie wymaga aktywnej ingerencji w system, nie może ono doprowadzić do zakłócenia pracy badanych urządzeń/systemu. Dopuszczenie do takich badań w pełnym lub ograniczonym zakresie (np. dla wybranych sieci, systemów czy urządzeń) pozostaje do decyzji Zamawiającego i każdorazowo przed rozpoczęciem badania jego zakres oraz możliwe skutki będą dyskutowane z przedstawicielem Zamawiającego.

Obecność administratora systemu będzie zapewniona przez cały czas realizacji zadań określonych. Natomiast wg ustaleń w przypadku nadmiernego ryzyka w zakresie aktywnej ingerencji należy przewidzieć przeprowadzenie audytu w formie pasywnego nasłuchiwania ruchu w wybranym punkcie systemu i wybranym oknie czasowym oraz późniejsza analiza tego ruchu. Aby takie nasłuchiwanie było możliwe konieczne jest skonfigurowanie w wybranych punktach sieci (na wybranych przełącznikach) funkcjonalności kopiowania ruchu z wybranego/wybranych portów na port nasłuchujący (funkcjonalność SPAN port/Port Mirroring). Konfiguracja tej funkcjonalności wymaga ingerencji administratora przełącznika.

**Audyt bezpieczeństwa, o którym mowa 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:
	1. certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu (każdy z audytorów powinien posiadać przynajmniej po jednym z wymienionych certyfikatów) **lub**
	2. co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, **lub**
	3. co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych
3. 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.