Szczegółowy opis przedmiotu zapytania ofertowego z dnia 04.10.2023 r.:

na przeprowadzenie Audytu bezpieczeństwa zgodnie z ZARZĄDZENIEM NR 8/2023/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 16 stycznia 2023 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców – ze zmianami (zwanego dalej: Zarządzeniem) w celu podniesienia bezpieczeństwa danych (cyberbezpieczeństwa) w Szpitalu Specjalistycznym Pro Familia Tomasz Łoziński sp. k.

Celem Audytu bezpieczeństwa zgodnie z ZARZĄDZENIEM NR 8/2023/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 16 stycznia 2023 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców – ze zmianami jest:

a) **wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z ZARZĄDZENIEM NR 8/2023/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 16 stycznia 2023 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców (ze zmianami**) w odniesieniu do stanu z przed wdrożenia działań podjętych przez Zamawiającego objętych Zapytaniami Ofertowymi ogłoszonymi na podstawie ww. Zarządzenia.

b) wydanie przez Zleceniobiorcę opinii na temat podniesienia poziomu bezpieczeństwa teleinformatycznego Zleceniodawcy oraz spełnienia warunków akceptacji zgodnie z § 3 Zarządzenia.

Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu z przed wdrożenia działań objętych ww. Zarządzeniem. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

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*.