Załącznik nr 1 do zaproszenia

AT.R.334.51.2023

Opis przedmiotu zamówienia

Nazwa zadania: „Przygotowanie audytu bezpieczeństwa teleinformatycznego Samodzielnego Publicznego Szpitala Wojewódzkiego im. Papieża Jana Pawła II w Zamościu”.

Kod CPV: 72254100-1 - Usługi w zakresie testowania systemu.

Przygotowanie audytu bezpieczeństwa teleinformatycznego Samodzielnego Publicznego Szpitala Wojewódzkiego im. Papieża Jana Pawła II w Zamościu

Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa wszystkich systemów teleinformatycznych wykorzystywanych przez Samodzielny Publiczny Szpital Wojewódzki im. Papieża Jana Pawła II w Zamościu.
Zakresem audytu należy objąć:

L.p.	Nazwa obszaru	Opis działań skutkujących podniesieniem bezpieczeństwa teleinformatycznego w Szpitalu
1.	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.
2.	Procesy zarządzania bezpieczeństwem informacji	-Nośniki wymienne - udokumentowany sposób postępowania -Zarządzanie tożsamością / dostęp do systemów w zakresie: -Przydzielanie i 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.
7.	Weryfikacja podniesienia poziomu bezpieczeństwa.	Przeprowadzony audyt wykazał podniesienie poziomu bezpieczeństwa teleinformatycznego w stosunku do stanu sprzed przystąpieniem do działań mających na celu podniesienie poziomu bezpieczeństwa teleinformatycznego finansowanych w ramach zarządzania.

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do przeprowadzenia testów bezpieczeństwa systemów informatycznych Zamawiającego zakończonych opracowaniem i dostarczeniem Raportów Testów Systemu. W raportach końcowych należy ująć szczegółowy opis obecnie funkcjonujących wszystkich elementów sieci teleinformatycznej oraz sporządzenie zaleceń obejmujących optymalizację, rozbudowę lub modernizację posiadanych rozwiązań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego w Szpitalu.
Dodatkowo audyt musi spełniać warunki określone w Zarządzeniu 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.

Opracował: Andrzej Szewczuk