Załącznik nr 1

Opis przedmiotu zamówienia w postępowaniu na wykonanie usługi pn.:

„Opracowanie planu działania i doradztwo w zakresie zakupu sprzętu IT oraz przygotowanie audytu bezpieczeństwa teleinformatycznego Samodzielnego Publicznego Szpitala Wojewódzkiego im. Papieża Jana Pawła II w Zamościu”.

Kod CPV: 72110000-9 Usługi doradcze w zakresie doboru sprzętu komputerowego.
Kod CPV: 72254100-1 - Usługi w zakresie testowania systemu.

Zadanie nr 1- Opracowanie planu działania i doradztwo w zakresie zakupu sprzętu IT.

Wykonanie następujących działań w zakresie poprawy cyberbezpieczeństwa infrastruktury IT Szpitala tj.:
- opracowanie planu działania w zakresie zakupu sprzętu IT, oprogramowania oraz usług gwarantujących podniesienie poziomu cyberbezpieczeństwa w Samodzielnym Publicznym Szpitalu Wojewódzkim im. Papieża Jana Pawła II w Zamościu, kwalifikujących się do sfinansowania ze środków określonych w ZARZĄDZENIU Nr 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r.
- przygotowanie opisu przedmiotu zamówienia do planowanych postępowań przetargowych wynikających z opracowanego planu zakupów,
- wsparcie podczas prowadzonych postępowań przetargowych na zakup ww. sprzętu oraz usług.

Zadanie nr 2 - 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	-Procedury zarządzania incydentami

	reagowanie na incydenty bezpieczeństwa	-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.

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 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.

Opracował: Andrzej Szewczuk