Szczegółowy opis przedmiotu zamówienia:

Przeprowadzenie audytów spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa.

1. Przeprowadzenie audytu zerowego

   Przeprowadzenie audytu zerowego w zakresie bezpieczeństwa i ciągłości funkcjonowania systemów informacyjnych służących do świadczenia usługi kluczowej w celu oceny stanu rzeczywistego w odniesieniu do wymagań określonych w ustawie o krajowym systemie cyberbezpieczeństwa, wydanych na jej podstawie rozporządzeń oraz wskazanych w nich polskich normach.

   Minimalny zakres audytu zerowego:

   - analiza i ocena dokumentacji w zakresie systemu zarządzania bezpieczeństwem informacji,
   - analiza dokumentacji systemu informatycznego,
   - weryfikacja przestrzegania dokumentacji zgodnie z zawartymi w nich zapisami,
   - przeprowadzenie wywiadów z wytypowanymi pracownikami poszczególnych komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa oraz wewnętrznych uregulowań w tym zakresie, w celu ustalenia faktów niezawartych lub niewynikających wprost z dokumentacji,
   - ocena zabezpieczeń fizycznych budynku oraz pomieszczeń,
   - analiza umów w zakresie bezpieczeństwa systemów teleinformatycznych,
   - ocena zarzadzania incydentami,
   - analiza procesu szacowania ryzyka,
   - analiza procesu kontroli dostępu do systemów teleinformatycznych,
   - analiza planu ciągłości działania,
   - nadzór nad zmianą.

   Przegotowanie raportu dotyczącego bezpieczeństwa audytowanych elementów wskazującego zidentyfikowane problemy oraz przedstawienie procedur naprawczych, jakie należy wykonać w celu usunięcia wskazanych w raporcie podatności. Prezentacja raportu oraz założeń realizowanych prac dla zarządu Szpitala oraz osób odpowiedzialnych za cyberbezpieczeństwo w WSS5.

2. Dostosowania WSS5 do wymogów ustawy o cyberbezpieczeństwie między innymi w zakresie:
   - **analiza krytyczności systemów** - analiza wykazu systemów informatycznych, oszacowanie krytyczności systemów wraz z ich powiązaniami w stosunku do procesów istotnych z punktu widzenia działalności Szpitala.
   - **opracowanie strategii bezpieczeństwa usług kluczowych** – zidentyfikowanie niezbędnych do realizacji projektów (jeżeli wymagane) dostosowujących Szpital do spełnienia wymagań zapewnienia bezpieczeństwa usług kluczowych. Zidentyfikowanie procesów niezbędnych do ustanowienia oraz formalnych dokumentów niezbędnych do opracowania i wdrożenia w organizacji, które będą stanowiły trzon zarządzania bezpieczeństwem i ciągłością usług.
   - **budowanie świadomości pracowników** - przygotowane szkolenia w formie e-learning, na autorskim systemie wykonawcy dedykowanym do prowadzenia szkoleń w zakresie bezpieczeństwa informacji, przygotowanie informacji w postaci prezentacji, newsletterów oraz materiałów informacyjnych.

     Przeprowadzenie szkolenia w siedzibie WSS5 dla pracowników szpitala w zakresie cyberbezpieczeństwa czas trwania ok 1,5 h. grupa ok 80 osób. Dokładny termin szkolenia do ustalenia z Zamawiającym. Zamawiający zapewnia salę wykładową oraz projektor.

- role i odpowiedzialności – wspólne z Zamawiającym zdefiniowanie ról z uprawnieniami oraz odpowiedzialnościami za poszczególne elementy w celu skutecznego wdrożenia i utrzymania zaprojektowanych procesów oraz ich doskonalenia.
- audyt teleinformatyczny – przeprowadzenie audytu bezpieczeństwa infrastruktury IT w celu oceny stosowanych zabezpieczeń przed wyciekiem danych lub w celu zachowania ciągłości funkcjonowania systemów informacyjnych służących do świadczenia usługi kluczowej. Przedstawienie rekomendacji jak bronić się przed zagrożeniami zidentyfikowanymi podczas przeprowadzonych audytów.

  Przedstawienie raportu prezentującego wyniki przeprowadzonych audytów teleinformatycznych opisującego wszystkie spostrzeżenia oraz zalecenia zmian konfiguracji systemów informatycznych.

  Minimalny zakres audytu teleinformatycznego:
  - API - testy bezpieczeństwa blackbox;
  - urządzenia sieciowe - zewnętrzny test bezpieczeństwa blackbox;
  - testy infrastruktury WAN;
  - testy penetracyjne sieci LAN;
  - testy socjotechniczne.

3. Przeprowadzenie audytu końcowego

   przeprowadzenie audytu końcowego – przeprowadzenie audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa poprzez weryfikację dokumentacji bezpieczeństwa oraz weryfikację zgodności technicznej systemów mających wpływ na świadczenie usługi kluczowej.

   Sporządzenie pisemnego sprawozdanie na podstawie zebranych przez audytorów dokumentów i dowodów z przeprowadzonego audytu i przekazanie ich operatorowi usługi kluczowej (Zamawiającemu) wraz z dokumentacją z przeprowadzonego audytu w celu przekazania przez Zamawiającego na wniosek do:

   1) organu właściwego do spraw cyberbezpieczeństwa;

   2) dyrektora Rządowego Centrum Bezpieczeństwa - w przypadku, gdy operator usługi kluczowej jest jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

   3) Szefa Agencji Bezpieczeństwa Wewnętrznego.

Wymagania dla audytorów (co najmniej dwóch audytorów)

- Posiadanie certyfikatu 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 (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
- Posiadanie certyfikatu 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;
- Posiadanie co najmniej trzyletniej praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych, lub co najmniej dwuletniej praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymowanie 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.

Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, uważa się udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;
2) przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;
3) przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

- Wdrożenie procedur oraz przeprowadzenie audytu z zakresu cyberbezpieczeństwa zgodnie z wymogami ustawy o krajowym systemie cyberbezpieczeństwa w co najmniej jednym podmiocie.
- Audytor jest obowiązany do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.
- Wymagania zgodne z wytycznymi Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Terminie realizacji:

Do dnia 18 maja 2020 roku.

Wymagane przedstawienie comiesięcznych raportów potwierdzających realizację usługi począwszy od dnia: 18 stycznia 2020, będących jednocześnie podstawą do wystawienia faktur.

Podstawowe informacje dotyczące Wojewódzkiego Szpitala Specjalistycznego nr 5 im. Św. Barbary w Sosnowcu:

1. Posiadane i utrzymane certyfikaty:
   - CERTYFIKAT ISO 9001: 2008 od 11.06.2012;
   - CERTYFIKAT ISO 14001: 2014; PN-N-18001:2014 od 11.06.2015;
   - CERTYFIKAT ISO/IEC 27001: 2013 od 13.07.2017;
   - Akredytacja od 27.02.2015.
2. Liczba lokalizacji: **1**
   [Wojewódzki Szpital Specjalistyczny nr 5 im. św. Barbary w Sosnowcu; Pl. Medyków 1; 41-200; Sosnowiec].
3. Ogólna liczba pracowników: **1 500 osób.**
4. Liczba pracowników IT (Obszar Zarządzania Informacją): **10 osób.**
5. Ilość systemów wykorzystywanych do świadczenia usługi kluczowej: **4.**
6. Liczba stanowisk komputerowych: **700.**
7. Liczba serwerów fizycznych: **21 (+ 7 serwerów monitoringu wizyjnego).**
8. Liczba serwerów wirtualnych: **27.**
9. Ilość serwerowni: **1.**
10. Ilość Access Point (WiFi): **120.**
11. Ilość podsieci: **4.**
12. Ilość adresów zewnętrznych: **3.**
13. Ilość switchy: **130.**
14. Firewall: **TAK.**

15. DHCP: TAK.
16. IPS: TAK.
17. VPN IPSsc: TAK.
18. VPN SSL (Open VPN): TAK.
19. Drukarki sieciowe: 30 sztuk.
20. Ilość urządzeń sieciowych (drukarki, routery, urządzenia VoIP etc.): 250.
21. Ilość stron internetowych: 1 (+ eRejestracja)
22. Active Directory: TAK.
23. Ochrona fizyczna i techniczna obiektów: Outsourcing. .

DYREKTOR
Wojewódzkiego Szpitala Specjalistycznego Nr 5
im. św. Barbary w Sosnowcu

dr n. med. Alicja Cegłowska