Załącznik nr 1 do SWZ - Szczegółowy opis przedmiotu zamówienia

Obszar 1

1.1. Przeprowadzenie wstępnego badania poziomu dojrzałości cyberbezpieczeństwa u Zamawiającego w terminie 14 dni od daty podpisania umowy oraz badania poziomu dojrzałości po wdrożeniu wybranych do realizacji przez Zamawiającego rekomendacji Wykonawcy wynikających z badania wstępnego w terminie nieprzekraczalnym do dnia 8 grudnia 2022 roku. Poniżej przedstawiono wymagania dotyczące rzeczonych badań:

- audyt wstępny bezpieczeństwa ma na celu dokonanie podsumowania stanu dojrzałości cyberbezpieczeństwa Zamawiającego w świetle obowiązujących przepisów prawa oraz wskazanie rekomendacji dla Zamawiającego, dotyczących wdrożenia niezbędnych w ocenie Wykonawcy zmian;
- audyt wstępny zostanie wykonany w taki sposób, aby umożliwić Zamawiającemu udokumentowanie zasadności planowanych zakupów inwestycyjnych ze środków finansowych Narodowego Funduszu Zdrowia, o których mowa 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;
- wykonawca przeprowadzi audyt powdrożeniowy, który będzie podstawą do oceny poprawy poziomu cyberbezpieczeństwa Zamawiającego, wynikającego z wdrożonych rekomendacji Wykonawcy;
- audytorzy oddelegowani przez Wykonawcę do czynności, wynikających z treści zamówienia, muszą posiadać wiedzę z zakresu przepisów dotyczących wymagań, zgodnie z treścią ustawy z dnia 1 7 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 1 2 kwietnia 201 2 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655);
- raport z audytu wstępnego musi zawierać wytyczne oraz sugestie związane z poprawą konkretnych obszarów cyberbezpieczeństwa, w tym rekomendacje rozwiązań technologicznych oraz organizacyjnych, potrzebnych do zabezpieczenia obszarów, w ramach których Wykonawca wskaże niski poziom dojrzałości cyberbezpieczeństwa Zamawiającego;

Powyższe badanie dojrzałości cyberbezpieczeństwa Zamawiającego musi być wykonane według następujących zasad:

- pytania zawarte w karcie audytowej badania dojrzałości muszą być zgodne z odpowiednimi zapisami występującymi w nst. normach: PN EN/ISO 27001:2021, PN EN/ISO 27002:2017, PN EN/ISO 27006:2021, PN EN/ISO 27701:2021, PN EN/ISO 27799:2016, PN EN/ISO 22301:2020.
- skala ocen badania dojrzałości musi być zgodna z normą ISO/IEC 21827.
- procedura badania dojrzałości cyberbezpieczeństwa musi być przeprowadzona zgodnie z wymogami normy PN EN/ISO 19011:2018.
- dodatkowe wymogi dla Wykonawców zawarte są w zarządzeniu nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.

Obszar 2

1.2. Opracowanie polityki i procedury systemu zarządzania ryzykiem w tym:

- opracowanie polityki i procedury systemu zarządzania ryzykiem;

- identyfikacja kluczowych procesów biznesowych oraz wspierających je zasobów informacyjnych, teleinformatycznych, organizacyjno-prawnych, osobowych i łańcucha dostaw wypracowanych wspólnie przez Wykonawcę z czynnym udziałem pracowników Zamawiającego;
- identyfikacja ryzyk usług kluczowych (udzielenie świadczeń zdrowotnych i gospodarka produktami leczniczymi i wyrobami medycznymi) w kontekście ustawy o krajowym systemie cyberbezpieczeństwa (KSC) we współpracy z Zamawiającym;
- opracowanie przez Wykonawcę metodyki szacowania ryzyka;
- nadzór Wykonawcy nad przeprowadzeniem przez pracowników Zamawiającego pierwszego oszacowania prawdopodobieństwa materializacji wystąpienia ryzyka oraz jego wpływu na prowadzenie biznesu;
- nadzór Wykonawcy nad przeprowadzaniem przez pracowników Zamawiającego analizy ryzyka, mającej na celu przygotowanie wniosków, które zawierają plany ograniczenia ryzyka wraz z propozycją konkretnych działań minimalizujących skutki wystąpienia ryzyka.

1.3. Opracowanie procedury monitorowania i obsługi incydentów w kontekście wymagań ustawy o KSC.

1.4. Opracowanie wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655), o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii wraz z asystą wdrożeniową w procesie wprowadzenia tej dokumentacji do stosowania.

Opracowanie dokumentacji SZBI obejmuje następujące dokumenty:

a) PBI – polityka zintegrowanego systemu zarzadzania;
b) PBI - księga zintegrowanego systemu zarzadzania;
c) Deklaracja stosowania;
d) Procedura - nadzór nad udokumentowanymi informacjami;
e) Procedura - audyt wewnętrzny;
f) Procedura - przegląd zarządzania;
g) Procedura - zarządzanie podatnościami;
h) Instrukcja - instrukcja zabezpieczania materiału dowodowego;
i) Rejestr - rejestr zdarzeń i incydentów (wzór);
j) Procedura - zarządzanie incydentami bezpieczeństwa;
k) Procedura - zarządzanie nośnikami informacji;
l) Procedura - zarządzanie bezpieczeństwem zasobów ludzkich;
m) Polityka dostępu do środowiska teleinformatycznego;
n) Polityka bezpieczeństwa informacji dla wykonawców zewnętrznych;
o) Procedura - działania korygujące;
p) Polityka pozyskiwania rozwoju i utrzymania systemów;
q) Procedura - monitorowanie skuteczności zintegrowanego systemu zarządzania;
r) Procedura - zarządzanie wyjątkami bezpieczeństwa informacji;
s) Słownik - słownik definicji i skrótów;
t) Procedura - zasady postepowania z informacjami – zmiany;
u) Polityka i metodyka zarządzania ryzykiem;
v) Polityka nadawania, odbierania, modyfikacji uprawnień;
w) Plan odtwarzania po awarii;
x) Opracowanie wzorów formularzy i rejestrów będących integralną częścią w/w dokumentów.

1.5. Asysta wdrożeniowa obejmuje:

a) 5 bloków szkoleniowych po 4 godziny lekcyjne (45 min) realizowanych w trybie on-line;

b) 60 godzin pracy certyfikowanych audytorów systemu zarządzania bezpieczeństwem informacji (zgodnie z ISO 27001 i 27799). Podstawową formą asysty wdrożeniowej jest praca zdalna (on-line).

1.6. Przeprowadzenie szkoleń dla kadry zarządzającej oraz osób zatrudnionych u Zamawiającego w zakresie podstawowej świadomości bezpieczeństwa informacji oraz cyberbezpieczeństwa , w tym:

Wymagany zakres szkolenia dla kadry zarządzającej Zamawiającego:

A. Cyberbezpieczeństwo w PWDL:

1) Cyberzagrożenia w Polsce;
2) Cyberbezpieczeństwo w ochronie zdrowia;
3) Wymagania ustawy o krajowym systemie cyberbezpieczeństwa (KSC);
4) Stopnie alarmowe i wynikające z nich obowiązki dla PWDL;
5) Kodeks Postępowania w Ochronie Zdrowia;
6) Wymagania Ustawy o Ochronie Danych Osobowych;
7) Prawa i obowiązki:
   a) Administratora Danych Osobowych (ADO);
   b) Inspektora Ochrony Danych (IOD);
   c) Oficera Bezpieczeństwa Informacji (OBI);
   d) Administratora Systemów Informatycznych (ASI);
   e) Forum Bezpieczeństwa.

B. Analiza ryzyka i zapewnienie ciągłości działania PWDL :

1) Procesy, procesy kluczowe i stopień ich krytyczności;
2) Parametry procesów;
3) Metodyka analiz ryzyka i ich wpływ na ciągłość działania;
4) Postępowanie z ryzykiem:
   a) planowanie i działania zaradcze,
   b) zarządzanie zmaterializowanym ryzykiem,
   c) analiza skutków oraz działania naprawcze i korygujące.

C. Obszary cybezpieczeństwa:

1) Ochrona prywatności i ochrona danych osobowych;
2) Bezpieczeństwo przetwarzania danych osobowych;
3) Ocena skutków dla ochrony danych;
4) Rejestr czynności przetwarzania i analiza DPIA;
5) Bezpieczeństwo informacji – podstawowe definicje;
6) Obszary analizy bezpieczeństwa informacji (organizacyjny, prawny, techniczny, ekonomiczny) w systemach informacyjnych;
7) Zarządzanie usługami IT/ICT – podstawowe definicje.

Minimalny czas szkolenia w powyższym zakresie powinien 4 godziny

Zakres szkolenia dla pracowników i współpracowników Zamawiającego:

A. Podstawowe zasady bezpiecznego korzystania z zasobów informacyjnych w cyberprzestrzeni:

1) Zabezpieczenia fizyczne dostępu do dokumentów, urządzeń i komputerów;
2) Hasła;
3) Użytkowanie sprzętu IT;
4) Oprogramowanie użytkowe;
5) Internet;
6) Poczta elektroniczna;
7) Praca zdalna;
8) instrukcja postępowania w przypadku wystąpienia incydentu;
9) System kopii bezpieczeństwa;

10) Systemy antywirusowe;
11) System zarządzania dostępem;
12) System EDR (Endpoint Detection and Response to narzędzie służące wykrywaniu i reagowaniu na podejrzane aktywności na urządzeniach końcowych).

B. Przykładowe zagrożenia w cyberprzestrzeni dla użytkowników zasobów informacyjnych:
1) Niekontrolowana utrata danych osobowych;
2) Hakowanie urządzeń IT/ICT i medycznych;
3) Wyłudzenia danych np. przez SMSy, maile;
4) Statystyki ataków hackerskich (np. wg Orange Tarcza);
5) Typy ataków z przykładami.

Wymagane jest przeprowadzenie tego szkolenia dla poszczególnych grup personelu PWDL, takich jak lekarze, pielęgniarki, personel techniczny…..
Zamawiający zapewni udział personelu w w/w szkoleniach
Czas trwania szkolenia: 3 godziny
Dopuszczalne są trzy formy prowadzenia szkolenia:
a) Stacjonarna – w siedzibie Zamawiającego;
b) Zdalna on-line.
c) Hybrydowa

Obszar 3

1.7. Przedmiotem zamówienia jest zakup kompleksowej usługi wdrożenia i doskonalenia u Zamawiającego systemu planowania i zarządzania ciągłością działania, opartego na analizie ryzyka ze szczególnym uwzględnieniem cyberbezpieczeństwa wspieranej systemem klasy ERM (Enterprise Risk Management), dedykowanym dla ochrony zdrowia.
Zakup licencji na używanie systemu klasy ERM wraz z usługą utrzymania.
Zakres prac musi obejmować:
1) zarządzanie ochroną prywatności (zgodnie z normami PN-EN/ISO 27701, 27707, 29134),
2) zarządzanie bezpieczeństwem informacji (zgodnie z normami PN-EN/ISO 27799, 27001, 27002, 27005,),
3) zarządzanie ciągłością działania (zgodnie z normami PN-EN/ISO 22301, 22313, 27031),
adekwatnie do zidentyfikowanych ryzyk u Zamawiającego.
Wymagany zakres prac:
1) Szkolenia z podstawowych zagadnień analizy ryzyka i ciągłości działania dla kadry kierowniczej i Zespołu Wdrożeniowego PWDL .
2) Instalacja wstępnie sparametryzowanego systemu klasy ERM u Zamawiającego.
3) Instruktaż w zakresie planowania i zarządzania ryzykiem z użyciem systemu klasy ERM dla oddelegowanego personelu Zamawiającego.
4) Parametryzacja systemu klasy ERM przez Zespół Wdrożeniowy pod nadzorem ekspertów Wykonawcy w zakresie:
a) Inwentaryzacji kluczowych zasobów osobowych, technicznych, informacyjnych i organizacyjno-prawnych oraz powiązania ich z predefiniowanymi procesami kluczowymi;
b) Przeprowadzenia analizy BIA (Business Impact Analysis/j. pol. analiza skutków na ciągłość działania) czyli określenia krytyczności procesów kluczowych oraz wpływu potencjalnych zagrożeń (zakłóceń, incydentów, katastrof) na utrzymanie ciągłości działania tych procesów;
c) Zdefiniowania scenariuszy ryzyka, zagrożeń i podatności dla zidentyfikowanych procesów krytycznych;
d) Przeprowadzenia analiz PRA (Process-oriented Risk Analysis - analiza ryzyka zorientowana na procesy) dla zidentyfikowanych procesów krytycznych;

e) Przypisania czynności przetwarzania dla zasobów zawierających dane osobowe, w tym szczególne dane medyczne;
f) Zidentyfikowania scenariuszy ryzyka dla zasobów powiązanych z czynnościami przetwarzania;
g) Przeprowadzenia analiz DPIA (Data Protection Impact Assessement - ocena skutków dla ochrony danych) dla zasobów zawierających dane osobowe lub szczególne dane medyczne;
h) Zgłaszania i obsługi incydentów.

5) Nadzór merytoryczny nad pracami Zespołu Wdrożeniowego związanymi z aktualizowaniem, uzupełnianiem i generowaniem brakującej dokumentacji: polityk, procedur, instrukcji, wzorów rejestrów i regulaminów.
6) Instruktaż użytkowników i koordynatorów kluczowych procesów. uczestniczących w planowaniu i zarządzaniu ryzykiem, w zakresie eksploatacji systemu klasy ERM.
7) Konsultacje w zakresie zaplanowanych audytów i doraźnych kontroli zewnętrznych.

Zamawiający wymaga przeznaczenia na konsultacje związane z realizacją prac określonych powyżej w punktach 5 i 7 minimum 50 godzin pracy ekspertów.

Zamawiający wymaga aby prace realizowane były pod kierownictwem co najmniej dwóch certyfikowanych audytorów :

1) Systemu Zarządzania Bezpieczeństwem Informacji;
2) Ochrony Prywatności;
3) Systemu Zarządzania Ciągłością Działania;
4) Zarządzania Usługami Teleinformacyjnymi.

Wymagany czas realizacji: do 30 listopada 2022 roku.

Obszar 4

1.8. Przeprowadzenie audytów spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa.

1.8.1. Przeprowadzenie audytu zerowego w zakresie bezpieczeństwa i ciągłości funkcjonowania systemów informacyjnych służących do świadczenia usług kluczowych w celu oceny stanu rzeczywistego w odniesieniu do wymagań określonych w Ustawie o KSC, 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.

Przygotowanie 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 Zamawiającego oraz osób odpowiedzialnych za cyberbezpieczeństwo u Zamawiającego.

1.8.2. Nadzór Wykonawcy nad dostosowaniem przez Zamawiającego infrastruktury krytycznej szpitala do wymogów Ustawy o KSC zgodnie z rekomendacjami Wykonawcy zawartymi w raporcie z audytu zerowego w zakresie uzgodnionym z Zamawiającym:

1.8.3. Przeprowadzenie audytu końcowego spełnienia wymagań Ustawy o KSC poprzez weryfikację dokumentacji bezpieczeństwa oraz weryfikacje zgodności technicznej systemów mających wpływ na świadczenie usług kluczowych.

Sporządzenie sprawozdania opracowanego zgodnie z wymaganym wzorem, opublikowanym przez ministra właściwego ds. cyberbezpieczeństwa na podstawie zebranych przez audytorów dokumentów i dowodów z przeprowadzonego audytu i przekazanie ich operatorowi usług kluczowych – Zamawiającemu.

Powyżej wymienione prace wchodzące w skład Obszaru 4 muszą się zakończone przedstawieniem Zamawiającemu raportu końcowego do dnia 31 maja 2023 roku.

Minimalne wymagania dla audytorów:

Zamawiający wymaga przeprowadzenia audytów spełnienia wymagań Ustawy o KSC przez co najmniej dwóch audytorów zatrudnionych przez Wykonawcę, posiadających certyfikaty w następujących zakresach:

a) audytor systemu zarządzania bezpieczeństwem informacji
b) audytor systemu zarządzania ciągłością działania
c) audytor systemu zarządzania usługami

wydanych 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;

Zamawiający wymaga dołączenia do oferty kopii wymaganych certyfikatów poświadczonych za zgodność z oryginałem.

Wykonawca zobowiązany jest do przedstawiania Zamawiającemu do zatwierdzenia raportów z wykonanych prac za każdy miesiąc kalendarzowy począwszy od stycznia 2023 roku. Zamawiający ma 7 dni kalendarzowych na zgłoszenie ewentualnych uwag i zatwierdzenie raportu. Zatwierdzony raport jest podstawą do wystawienia przez Wykonawcę faktury VAT Zamawiającemu.

1.8.4. Zakup usługi utrzymania systemu planowania i zarządzania ciągłością działania, opartego na analizie ryzyka ze szczególnym uwzględnieniem cyberbezpieczeństwa wspieranej systemem klasy ERM (Enterprise Risk Management), dedykowanym dla ochrony zdrowia za okres do 1 stycznia 2023 roku do dnia 31 grudnia 2024 roku. Usługa ta będzie płatna w ramach abonamentu miesięcznego.

Przedmiot zamówienia opisany w *Obszarze 4* będzie finansowany ze środków własnych Zamawiającego.

Podstawowe informacje dotyczące Szpitala Zamawiającego:

1) Posiadane i utrzymane certyfikaty:
   a. CERTYFIKAT: ISO 9001:2015
   b. ISO 15189:2006

   Akredytacja od : BRAK
2) Liczba lokalizacji: 1
3) Adresy lokalizacji: Szymanowskiego 11, Ostrowiec Świętokrzyski
4) Liczba pracowników IT (Obszar Zarządzania Informacją): 5
5) Ilość systemów wykorzystywanych do świadczenia usług kluczowych: 1
6) Nazwy i typy (HIS LIS RIS PACS) w/w systemów OPTIMED NXT, PROFLAB, ARPACS, ERP OPTIMED (systemy zintegrowane, traktowane jako 1 organizm usługi kluczowej)
7) Liczba stanowisk komputerowych ogółem: 345
8) Liczba stanowisk – komputery stacjonarne: 335
9) Liczba stanowisk – komputery przenośne: 10

10) Liczba stanowisk – tablety: 20
11) Liczba stanowisk – smartfony: 0
12) Liczba serwerów fizycznych: 22
13) Liczba serwerów monitoringu wizyjnego: 2
14) Liczba serwerów wirtualnych: 16
15) Ilość serwerowni: 1
16) Ilość Access Point (WiFi): 50
17) Ilość podsieci: 17
18) Ilość adresów zewnętrznych: 2
19) Ilość switchy: 31
20) Firewall (TAK/NIE): TAK
21) DHCP (TAK/NIE): TAK
22) IPS (TAK/NIE): TAK
23) VPN IPsec (TAK/NIE): TAK
24) VPN SSL (open VPN) (TAK/NIE): TAK
25) Drukarki sieciowe: 118 sztuk.
26) Ilość urządzeń sieciowych zarządzanych (routery, urządzenia VolP etc.): 348
27) Ilość stron internetowych: 1 ZEWNĘTRZNA, 1 WEWNĘTRZNA, BIP
28) Active Directory (TAK/NIE): TAK
29) Ochrona fizyczna i techniczna obiektów (wew./Outsourcing): OUTSOURCING