**Załącznik nr 5**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zadanie nr 3 - Działania zwiększające poziom cyberbezpieczeństwa szpitala**

**3a) System zarządzania bezpieczeństwem informacji – 1 sztuka (zestaw)**

Przedmiotem zamówienia jest opracowanie, wdrożenie oraz utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Mazowieckim Szpitalu Onkologicznym w Wieliszewie, zgodnego z wymaganiami normy PN-EN ISO/IEC 27001:2022 lub równoważną normą/standardem w zakresie SZBI.

Celem wdrożenia jest zapewnienie skutecznego i zgodnego z normą systemu zarządzania bezpieczeństwem informacji, obejmującego procesy, procedury, zasoby i środki techniczne mające na celu ochronę poufności, integralności i dostępności informacji przetwarzanych w Szpitalu.

Producent (marka) …………………………………..…………………..……(Należy podać)

Model ……………………………………………………..………………… (Należy podać)

Kraj pochodzenia .…………………………………..…………….………… (Należy podać)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | W ramach realizacji zamówienia Wykonawca zobowiązuje się do: |  |  |
|  | **Analizy stanu obecnego**   * + Przeprowadzenie audytu wstępnego w zakresie bezpieczeństwa informacji i opracowanie raportu z audytu;   + Ocena zgodności z wymaganiami PN-EN ISO/IEC 27001:2022;   + Analiza istniejących polityk, procedur, środków i procesów bezpieczeństwa informacji w Szpitalu | Tak |  |
|  | **Pomoc w identyfikacji aktywów informacyjnych**   * Określenie aktywów (w tym: systemów informatycznych, dokumentów, zasobów) mających kluczowe znaczenie dla bezpieczeństwa informacji; * Określenie znaczenia aktywów informacyjnych dla bezpieczeństwa informacji; * Określenie właścicieli aktywów informacyjnych; * Określenie umiejscowienia aktywów informacyjnych. | Tak, podać |  |
|  | **Ocena ryzyka związanego z bezpieczeństwem informacji** z uwzględnieniem wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r oraz wytycznych określonych w normie ISO 31000:   * Ocena ryzyka; * Opracowanie planu postępowania z ryzykiem, obejmującego działania minimalizujące ryzyka istotne dla Szpitala. | Tak |  |
|  | **Przeprowadzenia klasyfikacji informacji**   * Opracowanie zasad klasyfikacji informacji zgodnych z wymaganiami normy ISO/IEC 27001:2022. | Tak |  |
|  | **Określenie celów bezpieczeństwa informacji i opracowanie planu realizacji celów bezpieczeństwa informacji**   * Zdefiniowanie celów bezpieczeństwa informacji oraz opracowanie planu ich realizacji. | Tak |  |
|  | **Opracowanie dokumentacji SZBI**  Wykonawca opracuje kompletny zestaw dokumentów SZBI zgodnych z wymaganiami normy ISO/IEC 27001:2022, w tym:   * Politykę bezpieczeństwa informacji; * Deklarację stosowania zabezpieczeń; * Polityki, procedury i instrukcje dotyczące m.in.:   - organizacji bezpieczeństwa informacji;  - zarządzania aktywami i klasyfikacji informacji;  - zarządzania ryzykiem;  - zarządzania dostępem użytkowników;  - bezpieczeństwa kryptograficznego;  - bezpieczeństwa fizycznego i środowiskowego;  - bezpieczeństwa sprzętu i eksploatacji;  - bezpieczeństwa komunikacji;  - pozyskiwania, rozwoju i utrzymania systemów informacyjnych;  - bezpieczeństwa w relacjach z dostawcami;  - zarządzania incydentami bezpieczeństwa informacji;  - zarządzania ciągłością działania;  - zapewnienia zgodności z wymaganiami prawnymi i normatywnymi;  - monitorowania i pomiaru skuteczności SZBI. | Tak |  |
|  | **Wdrożenia SZBI**   * + Szkolenie dla personelu z zakresu wymagań i stosowania dokumentacji systemu zarządzania bezpieczeństwem informacji   + Wsparcie doradcze w procesie wdrażania systemu (konsultacje stacjonarne – 2 razy w miesiącu przez okres wdrożenia ). | Tak |  |
|  | **Utrzymania SZBI (w okresie 36 miesięcy)**   * + Monitorowanie skuteczności funkcjonowania systemu   + Wsparcie w cyklicznym szacowaniu i przeglądzie ryzyk cyberbezpieczeństwa   + Wsparcie w doskonaleniu systemu i audytach okresowych   + Wsparcie w zakresie monitorowania bezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług   + Wsparcie w nadzorowaniu incydentów bezpieczeństwa informacji / cyberbezpieczeństwa   + Wsparcie w opracowywaniu i testowaniu planów ciągłości działania (BCP) i planów odtwarzania (DRP)   + Prowadzenie szkoleń dla audytorów wewnętrznych systemu zarządzania bezpieczeństwem informacji   + Pomoc w aktualizacji analizy kontekstu   + Pomoc w identyfikacji i aktualizacji wykazu aktywów informacyjnych   + Pomoc w przygotowaniu programów audytów wewnętrznych   + Ocena stosowanych zabezpieczeń teleinformatycznych   + Opiniowanie zabezpieczeń teleinformatycznych   + Pomoc w określaniu priorytetów i celów bezpieczeństwa informacji   + Wsparcie w kontaktach z jednostką certyfikującą oraz uczestniczenie w audytach prowadzonych przez jednostkę certyfikującą system zarządzania bezpieczeństwem informacji   + Udział w realizacji działań korygujących   + Pomoc w przygotowaniu, przeprowadzaniu i dokumentowaniu przeglądów zarządzania | Tak |  |
|  | **Wymagania wobec wykonawcy**  Wykonawca powinien:   * Posiadać co najmniej dwuletnie doświadczenie w realizacji projektów wdrożenia SZBI zgodnych z normą ISO/IEC 27001:2022; * Wykazać się realizacją co najmniej 4 wdrożeń SZBI zgodnych z normą ISO/IEC 27001:2022; * Dysponować zespołem co najmniej 2 audytorów, posiadających certyfikaty Audytora Wiodącego ISO/IEC 27001:2022, zgodnych z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu; * Posiadać aktualne ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności. | Tak |  |

3b) **Szkolenia dla kadry kierowniczej z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny) – 5 sztuk**

Przedmiotem zamówienia jest przeprowadzenie Szkolenia dla kadry kierowniczej z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

CEL SZKOLENIA:

Celem szkolenia jest wyposażenie kadry kierowniczej oraz administratorów systemów w praktyczną wiedzę i umiejętności niezbędne do skutecznego przeciwdziałania incydentom bezpieczeństwa, a także wspierania kultury cyberbezpieczeństwa w organizacji**.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | FORMA REALIZACJI |  |  |
|  | * Tryb: szkolenie stacjonarne * Czas trwania: 1 dzień = ok 4 godziny zegarowe * Lokalizacja: siedziba Zamawiającego * Grupa docelowa: kadra kierownicza, administratorzy IT, osoby odpowiedzialne za bezpieczeństwo informacji w szpitalu | Tak |  |
|  | ZAKRES MERYTORYCZNY SZKOLENIA: |  |  |
|  | Podstawy prawne w obszarze cyberbezpieczeństwa   * Obowiązujące regulacje krajowe i unijne (w tym Ustawa o Krajowym Systemie Cyberbezpieczeństwa, RODO, KRI, NIS2) * Obowiązki podmiotów publicznych * Odpowiedzialność kadry kierowniczej za zapewnienie bezpieczeństwa | Tak |  |
|  | Podstawowe zasady cyberhigieny   * Dobre praktyki w codziennym użytkowaniu systemów informatycznych * Bezpieczne hasła, uwierzytelnianie, aktualizacje oprogramowania * Zarządzanie urządzeniami mobilnymi i zdalnym dostępem | Tak |  |
|  | Wybrane metody ataków – przegląd i analiza (z elementami Case Study)   * Phishing, ransomware, ataki typu DDoS, inżynieria społeczna   Analiza rzeczywistych przypadków ataków – jak do nich doszło i jak można było im zapobiec | Tak |  |
|  | Testy bezpieczeństwa   * Wprowadzenie do testów bezpieczeństwa - najważniejsze zagadnienia * Testy bezpieczeństwa w strategii organizacji * Ryzyka związane z brakiem testowania organizacji | Tak |  |
|  | Reagowanie na incydenty bezpieczeństwa   * Etapy obsługi incydentu: identyfikacja, eskalacja, reakcja, raportowanie * Rola administratorów i menedżerów w zarządzaniu kryzysowym * Komunikacja wewnętrzna i zewnętrzna w sytuacji wystąpienia incydentu | Tak |  |
|  | Rola kadry zarządzającej w budowaniu systemu bezpieczeństwa   * Kultura organizacyjna oparta na bezpieczeństwie * Polityki i procedury bezpieczeństwa – jak je tworzyć i nadzorować * Współpraca z działem IT i zewnętrznymi podmiotami | Tak |  |
|  | CERTYFIKATY: |  |  |
|  | Każdy uczestnik otrzyma imienny certyfikat ukończenia szkolenia, potwierdzający nabyte kompetencje z zakresu cyberbezpieczeństwa | Tak |  |
|  | WYMAGANIA WOBEC WYKONAWCY W ZAKRESIE SZKOLEŃ: |  |  |
|  | Wykonawca powinien:   * Posiadać co najmniej dwuletnie doświadczenie w realizacji szkoleń z zakresu cyberbezpieczeństwa oraz bezpieczeństwa informacji; * Wykazać się realizacją co najmniej 4 szkoleń w zakresie cyberbezpieczeństwa dla co najmniej 50 osób; * Posiadać aktualne ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności | Tak |  |

3c) **Szkolenia dla kadry biurowej i medycznej z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny) – 250 sztuk**

Przedmiotem zamówienia jest przeprowadzenie szkolenia dla kadry biurowej i medycznej z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny).

Szkolenie ma na celu podniesienie świadomości wszystkich pracowników szpitala w zakresie zagrożeń cyfrowych oraz ukształtowanie bezpiecznych nawyków pracy z systemami teleinformatycznymi**.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | FORMA SZKOLENIA: |  |  |
|  | * Tryb: szkolenie stacjonarne * Czas trwania: 1 dzień = ok 4 godziny zegarowe * Lokalizacja: siedziba Zamawiającego * Uczestnicy: wszyscy pracownicy szpitala – niezależnie od stanowisk | Tak |  |
|  | ZAKRES MERYTORYCZNY SZKOLENIA: |  |  |
|  | Wprowadzenie do cyberbezpieczeństwa   * Czym jest cyberbezpieczeństwo * Rola człowieka jako najsłabszego i zarazem najważniejszego ogniwa w systemie bezpieczeństwa * Konsekwencje naruszeń: przykłady incydentów z sektora ochrony zdrowia * Wymagania prawne: RODO, ustawa o Krajowym Systemie Cyberbezpieczeństwa, KRI | Tak |  |
|  | Najczęstrze cyberzagrożenia w ochronie zdrowia   * Phishing jak rozpoznać fałszywą wiadomość e-mail lub SMS * Ataki typu ransomware – blokowanie systemów i żądanie okupu * Inżynieria społeczna – manipulacja psychologiczna wobec pracownika * Podszywanie się pod zaufane osoby (spoofing) * Złośliwe oprogramowanie – jak może trafić do komputera szpitalnego * Kradzież danych przez urządzenia zewnętrzne (pendrive, smartfon) | Tak |  |
|  | Cyberhigiena – codzienne nawyki bezpieczeństwa |  |  |
|  | * Silne i bezpieczne hasła – jak je tworzyć i zarządzać nimi * Zasady korzystania z poczty służbowej * Bezpieczne przeglądanie stron internetowych * Zakazy i ograniczenia – czego nie wolno robić na komputerach służbowych * Bezpieczne przesyłanie dokumentów (np. wyników badań, historii choroby) * Korzystanie z urządzeń osobistych w pracy (BYOD – Bring Your Own Device) | Tak |  |
|  | Obsługa incydentów – co zrobić, gdy coś się dzieje? |  |  |
|  | * Czym jest incydent bezpieczeństwa i jak go rozpoznać * Najczęstsze objawy zagrożeń: dziwne wiadomości, spowolnienie sprzętu, podejrzane komunikaty * Kogo powiadomić i jak zgłosić incydent – łańcuch reakcji w szpitalu * Czego nie robić, gdy doszło do naruszenia | Tak |  |
|  | CERTYFIKATY: |  |  |
|  | Każdy uczestnik otrzyma imienny certyfikat ukończenia szkolenia, potwierdzający nabyte kompetencje z zakresu cyberbezpieczeństwa | Tak |  |
|  | WYMAGANIA WOBEC WYKONAWCY W ZAKRESIE SZKOLEŃ: |  |  |
|  | Wykonawca powinien:   * Posiadać co najmniej dwuletnie doświadczenie w realizacji szkoleń z zakresu cyberbezpieczeństwa oraz bezpieczeństwa informacji; * Wykazać się realizacją co najmniej 4 szkoleń w zakresie cyberbezpieczeństwa dla co najmniej 50 osób; * Posiadać aktualne ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności | Tak |  |