

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

Załącznik Nr 2 Opis przedmiotu zamówienia

Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji oraz przeprowadzenie szkoleń z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

1. Wprowadzenie

Zamówienie realizowane jest w ramach projektu pn. „Transformacja cyfrowa Szpitala Wielospecjalistycznego w Jaworznie – integracja systemów, digitalizacja dokumentacji i wzrost cyberbezpieczeństwa”, objętego wsparciem z Krajowego Planu Odbudowy i Zwiększania Odporności, inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”, nabór nr KPOD.07.03-IP.10-001/25.

Zakres przedmiotu zamówienia jest zgodny z dokumentacją inwestycji KPO dostępną na stronie internetowej [inwestycji D.1.12](#).

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

2. Przedmiot i cel zamówienia

1. Przedmiot zamówienia

Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz przeprowadzenie szkoleń z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny) w Szpitalu Wielospecjalistycznym w Jaworznie.

Przedmiot zamówienia obejmuje opracowanie dokumentacji i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji uwzględniającego kontekst organizacyjny Zamawiającego, w celu osiągnięcia zgodności funkcjonowania Szpitala z wymogami:

- Polskiej Normy PN-EN ISO/IEC 27001,
- rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI),
- ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), z uwzględnieniem jej aktualnych oraz potencjalnych zmian legislacyjnych w okresie realizacji zamówienia,
- przepisów ustawy o ochronie danych osobowych i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),

w zakresie obejmującym co najmniej procesy i usługi świadczone przez Zamawiającego. Zamówienie obejmuje również przeszkolenie personelu związane z wdrożeniem oraz stosowaniem udokumentowanego SZBI a także z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa. Zamawiający nabywa pełne autorskie prawa majątkowe do opracowanej dokumentacji SZBI z prawem do jej dalszej modyfikacji i dostosowywania do zmian organizacyjnych i prawnych.

Zakres i realizacja Przedmiotu Zamówienia przebiegać będzie z podziałem na 3 etapy:

- Etap 1: Analiza ryzyka i audyt obszaru bezpieczeństwa informacji (w celu ustalenia stanu obecnego).
- Etap 2: Opracowanie, przekazanie i wdrożenie pełnej dokumentacji systemu SZBI.
- Etap 3: Szkolenie personelu związane z wdrożeniem i stosowaniem SZBI oraz podnoszeniem świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

2. Cel zamówienia

Celem zadania jest znaczące podniesienie poziomu cyberbezpieczeństwa Szpitala Wielospecjalistycznego w Jaworznie poprzez wdrożenie kompleksowych rozwiązań organizacyjnych i edukacyjnych w zakresie ochrony systemów informatycznych, danych medycznych oraz infrastruktury szpitalnej, w tym:

- a) ustanowienie i wdrożenie skutecznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z obowiązującymi w tym zakresie przepisami i normami;
- b) wzmocnienie kompetencji zespołu ds. bezpieczeństwa informacji;
- c) zwiększenie poziomu cyberbezpieczeństwa Szpitala w zakresie organizacyjnym i technicznym;
- d) zapewnienie zgodności z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa;
- e) przygotowanie jednostki do audytu bezpieczeństwa potwierdzającego zabezpieczenie przetwarzania Elektronicznej Dokumentacji Medycznej (EDM), zgodnie z wymaganiami inwestycji KPO D1.1.2

3. Etapy i zakres realizacji usług

1. Etap 1 - Analiza ryzyka i audyt obszaru bezpieczeństwa informacji.

1. Wykonawca dokona analizy stanu obecnego technicznego i organizacyjnego, w tym posiadanej przez Zamawiającego dokumentacji oraz analizy ryzyk związanych z przetwarzaniem informacji i funkcjonowaniem systemów informatycznych, w tym infrastruktury medycznej i administracyjnej.
2. Wykonawca przeprowadzi analizę ryzyka informacji w środowisku Szpitala wraz z inwentaryzacją aktywów związanych z przetwarzaniem informacji i ich klasyfikacją.
3. Wykonawca wykona audyt obszaru bezpieczeństwa informacji obejmującego:
 - a) Klasyfikacja podmiotu względem ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz.U. 2018, poz. 1560, z późn.zm.)
 - b) Analiza stanu gotowości podmiotu względem KSC;

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

- c) Przegląd istniejącej dokumentacji i procesów w obszarze bezpieczeństwa informacji oraz stosowanych zabezpieczeń bezpieczeństwa informacji, procesów zarządzania ryzykiem i audytowania względem wymagań polskich norm PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005;
 - d) Przegląd obecnej dokumentacji i procesów w obszarze ciągłości działania, względem wymagań polskich norm PN-EN ISO 22301, PN-EN ISO 22313;
 - e) Przegląd obecnej dokumentacji w obszarze Ochrony Danych Osobowych względem ustawy RODO;
 - f) Przegląd polityki tworzenia i testowania kopii zapasowych względem rekomendacji Ministerstwa Zdrowia oraz rekomendacji Centrum e-Zdrowia;
 - g) Przegląd stosowanych w Szpitalu rozwiązań zabezpieczeń;
 - h) Badanie zgodności dokumentacji i procesów w obszarze bezpieczeństwa informacji względem Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (dalej „Rozporządzenie KRI”).
 - i) Szacowanie ryzyka, które umożliwi identyfikację ryzyka w obszarze technicznym (systemy, narzędzia i zasoby umożliwiające przetwarzanie informacji), organizacyjnym (procesy przetwarzania informacji oraz zapewnienia ciągłości działania), zasobów ludzkich (osoby przetwarzające informacje).
4. Wykonawca przedstawi wyniki analizy ryzyka i audytu oraz sporządzone w oparciu o niego rekomendacje w postaci jednolitego i spójnego raportu wraz z załączonymi wynikami szczegółowymi poszczególnych badań oraz opracowań zrealizowanych w ramach audytu.

2. Etap 2 – Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

1. Wykonawca przy współudziale Zamawiającego dokona:

- a) opracowania, aktualizacji oraz wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z elementami ciągłości działania w bezpieczeństwie informacji w oparciu o normę ISO 22301, uwzględniający kontekst organizacyjny Zamawiającego, w celu osiągnięcia zgodności z polskimi normami PN-EN ISO/IEC 27001 i PN-EN ISO/IEC 27002, Rozporządzeniem KRI, UKSC2 oraz RODO, jak również zgodnie z wymaganiami

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

inwestycji KPO D1.1.2. Zadanie dotyczy w szczególności opracowania, uzupełnienia, aktualizacji lub integracji dokumentacji min. w zakresie bezpieczeństwa informacji:

- 1) Metodyka identyfikacji, szacowania i postępowania z ryzykiem;
- 2) Analiza ryzyka;
- 3) Polityka bezpieczeństwa informacji;
- 4) Deklaracja stosowania ISO 27001;
- 5) Polityka bezpieczeństwa organizacyjnego;
- 6) Polityka bezpieczeństwa systemów teleinformatycznych;
- 7) Polityka bezpieczeństwa pracowniczego;
- 8) Polityka bezpieczeństwa fizycznego i środowiskowego;
- 9) Polityka ochrony danych osobowych;
- 10) Analiza BIA;
- 11) Polityka ciągłości działania;
- 12) Wymagane polityki, procedury, regulaminy i instrukcje niższego poziomu powiązane z w/w dokumentami, w szczególności polityki określone w wymogach inwestycji KPO:
 - a. Polityka zarządzania dostępem i uprawnieniami;
 - b. Polityka kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania;
 - c. Politykę zarządzania podatnościami;
 - d. Politykę zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa;
 - e. Politykę logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny;
 - f. Politykę kopii bezpieczeństwa;
 - g. Politykę zarządzania incydentami bezpieczeństwa;

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

- h. Politykę zarządzania ciągłością działania;
 - i. Politykę ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych.
-
- b) przeglądu i aktualizacji polityk ochrony danych osobowych pod kątem integracji i dostosowania do wymogów SZBI i RODO;
 - c) wsparcia we wdrożeniu opracowanej dokumentacji i procedur w organizacji szpitala;
 - d) wsparcia w określeniu ról i utworzeniu wewnętrznej struktury organizacyjnej bezpieczeństwa informacji (m.in. wyznaczenie Pełnomocnika ds. SZBI, Administratorów bezpieczeństwa, Zespołu reagowania na incydenty);
 - e) wsparcia w implementacji procedur zarządzania ryzykiem, incydentami i ciągłością działania;
 - f) Wykonawca zapewni wsparcie doradcze w zakresie wdrożenia polityk technicznych bezpieczeństwa, w tym opracowanie rekomendacji konfiguracyjnych dla istniejących systemów zabezpieczeń, bez wykonywania zmian konfiguracyjnych w środowisku produkcyjnym.
 - g) Wykonawca przygotuje listę wymagań związanych z bezpieczeństwem informacji oraz listę środków technicznych dla zapewnienia bezpieczeństwa informacji z uwzględnieniem środków aktualnie wykorzystywanych przez Zamawiającego
-
- ### 3. Etap 3 - Szkolenie personelu związane z wdrożeniem i stosowaniem SZBI oraz podnoszeniem świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)
-
1. Wykonawca zapewni szkolenia dla kadry kierowniczej Zamawiającego, a także dla minimum 75% pracowników biurowych oraz medycznych. Szkolenia mają odbywać się w siedzibie Zamawiającego. Zamawiający udostępni pomieszczenie wyposażone w rzutnik oraz dostęp do Internetu, na potrzeby szkolenia stacjonarnego. Każde szkolenie powinno trwać od 2 do 4 godzin szkoleniowych dla 1 grupy szkoleniowej w ciągu dnia. Liczba osób uczestniczących w szkoleniu nie przekroczy 80 osób na grupę. Szkolenia będą odbywać się w dni robocze od poniedziałku do piątku w godzinach 7.30 – 14.30 w siedzibie Zamawiającego. Wykonawca powinien również dostarczyć platformę umożliwiającą prowadzenie szkoleń i być gotowym do organizacji szkolenia online. Wykonawca zapewni prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób.

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

2. Szkolenia mają obejmować w szczególności:

- a) zasady funkcjonowania SZBI oraz stosowanie opracowanych polityk i procedur bezpieczeństwa informacji,
- b) role, obowiązki i odpowiedzialność członków zespołu ds. bezpieczeństwa informacji,
- c) proces przeglądu zarządczego SZBI, w tym cykl aktualizacji i doskonalenia systemu,
- d) proces zarządzania ryzykiem, incydentami i ciągłością działania,
- e) prowadzenie i aktualizacja rejestrów bezpieczeństwa informacji oraz dokumentowanie działań i incydentów,
- f) wymogi raportowania oraz dokumentowania przeglądów SZBI sposoby
- g) współpraca z personelem medycznym oraz Działem Informatyki w zakresie reagowania na incydenty bezpieczeństwa,
- h) bezpieczeństwo informacji nieelektronicznych oraz przetwarzanych poza systemami teleinformatycznymi (bezpieczeństwo fizyczne),
- i) omówienie obowiązujących regulacji, standardów, norm i dobrych praktyk w obszarze bezpieczeństwa teleinformatycznego, w tym: RODO, Dyrektywa NIS2, ustawa o Krajowym Systemie Cyberbezpieczeństwa, KRI, normy ISO/IEC 27001 i ISO 22301 lub równoważne,
- j) omówienie mechanizmów kontrolnych SZBI i Systemu Zarządzania Ciągłością Działania (SZCD),
- k) rola kierownictwa w zapewnianiu i nadzorze nad bezpieczeństwem informacji oraz infrastrukturą krytyczną,
- l) przegląd rozwiązań ochronnych, detekcyjnych i prewencyjnych w obszarze cyberbezpieczeństwa,
- m) skuteczne reagowanie na incydenty oraz przywracanie ciągłości działania po ataku.
- n) zasady przygotowania, prowadzenia i dokumentowania audytów wewnętrznych SZBI, w tym planowanie audytów, metodyka ich realizacji, raportowanie wyników oraz formułowanie działań korygujących.

3. Szkolenia kadry kierowniczej, co najmniej z zakresu:

- a) Podstaw prawnych w obszarze cyberbezpieczeństwa.
- b) Typów ataków wraz z przykładami
- c) Reagowania na incydenty.
- d) Wykonywania testów bezpieczeństwa.

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

e) Roli kadry zarządzającej w budowie kultury bezpieczeństwa.

4. Szkolenia pracowników administracji i pracowników medycznych, co najmniej z zakresu:

- a) Zasad cyberhigieny.
- b) Identyfikacji zagrożeń
- c) Reagowania na incydenty
- d) Odpowiedzialności prawnej

5. Szkolenie z ochrony przed wyłudzeniem osobowych i informacji, co najmniej z zakresu:

1. Wprowadzenie do Bezpieczeństwa Informacji

- a) Cel i znaczenie szkolenia
- b) Przegląd zagrożeń cybernetycznych
- c) Podstawowe zasady bezpieczeństwa informacji

2. Wykrywanie Phishingu oraz jego odmian

- a) Definicja i rodzaje phishingu (email, SMS, spear phishing, whaling)
- b) Metody rozpoznawania phishingu
- c) Przykłady ataków phishingowych
- d) Praktyczne ćwiczenia w wykrywaniu phishingu

3. Wykorzystywanie Mechanizmów Podwójnego Uwierzytelnienia (2FA)

- a) Co to jest podwójne uwierzytelnienie (2FA) i dlaczego jest ważne
- b) Rodzaje 2FA (SMS, aplikacje uwierzytelniające, tokeny sprzętowe)
- c) Konfiguracja 2FA na popularnych platformach
- d) Ćwiczenia praktyczne: wdrażanie i używanie 2FA

4. Stosowanie VPN

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

- a) Co to jest VPN i jak działa
 - b) Korzyści z używania VPN
 - c) Przegląd popularnych usług VPN
 - d) Praktyczne ćwiczenia: konfiguracja i korzystanie z VPN
5. Stosowanie SSL/TLS
- a) Podstawy SSL/TLS: co to jest i jak działa
 - b) Rola certyfikatów SSL/TLS
 - c) Jak sprawdzić poprawność certyfikatów SSL/TLS na stronach internetowych
 - d) Praktyczne ćwiczenia: konfiguracja SSL/TLS na serwerze
6. Rozpoznawanie Fałszywych Stron i Domen (Typosquatting, Punycod i ich Odmiany)
- a) Co to jest typosquatting i punycod
 - b) Techniki rozpoznawania fałszywych stron i domen
 - c) Narzędzia do weryfikacji domen i URL
 - d) Praktyczne ćwiczenia: identyfikacja fałszywych stron
7. Obrona przed Fałszywymi Sieciami WiFi
- a) Zagrożenia związane z fałszywymi sieciami WiFi (evil twin, rogue AP)
 - b) Jak rozpoznać i unikać fałszywych sieci WiFi
 - c) Narzędzia i techniki zabezpieczania się przed fałszywymi sieciami
8. Bezpieczeństwo w Użytkowaniu Sztucznej Inteligencji
- a) Wprowadzenie do sztucznej inteligencji i jej zastosowań
 - b) Zagrożenia związane z wykorzystaniem AI (deepfake, automatyzacja ataków)
 - c) Najlepsze praktyki w bezpiecznym używaniu AI
 - d) Przykłady narzędzi i rozwiązań wspierających bezpieczeństwo AI

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

6. Szkolenie ze stosowania i budowania silnych haseł, wykorzystywania menadżerów haseł oraz szyfrowania danych osobowych, co najmniej z zakresu:

1. Skuteczne Tworzenie Haseł
 - a) Zasady tworzenia silnych haseł
 - b) Częste błędy przy tworzeniu haseł
 - c) Narzędzia do generowania silnych haseł
 - d) Praktyczne ćwiczenia: tworzenie i ocena haseł
2. Skuteczne Szyfrowanie Danych
 - e) Podstawy szyfrowania danych: symetryczne i asymetryczne
 - f) Najlepsze praktyki szyfrowania danych w spoczynku i w tranzycie
 - g) Przykłady narzędzi do szyfrowania danych (VeraCrypt, BitLocker, PGP)
 - h) Ćwiczenia praktyczne: szyfrowanie i deszyfrowanie plików
3. Wykorzystywanie Menedżerów Haseł
 - i) Dlaczego menedżery haseł są ważne
 - j) Przegląd popularnych menedżerów haseł (LastPass, 1Password, Bitwarden)
 - k) Jak bezpiecznie korzystać z menedżerów haseł
 - l) Praktyczne ćwiczenia: zakładanie kont i korzystanie z menedżerów haseł
 - m) Świadomość zagrożeń — phishing, ransomware i socjotechnika
 - n) Procedury postępowania w przypadku podejrzenia incydentu bezpieczeństwa
 - o) Podsumowanie i najlepsze praktyki ochrony sprzętu prywatnego

7. Wykonawca powinien dostarczyć platformę szkoleniową (e-learning) o co najmniej funkcjonalności opisanej poniżej:

- a) Usługa dla min. 1000 użytkowników dostępna przez 36 miesięcy

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

- b) min. 15 szkoleń PL/EN w formie interaktywnych prezentacji, quizów oraz testów wiedzy w zakresie tematycznym uzgodnionym z Zamawiającym
 - c) Tematyka: phishing, malware, RODO, hasła, spam, bezpieczny Internet, bezpieczna praca zdalna, podstawy IT
 - d) Podział użytkowników na grupy i przypisywanie im szkoleń
 - e) Łączny czas materiałów min. 3 godziny
 - f) Platforma LMS + spersonalizowane ścieżki szkoleniowe
 - g) Powiadomienia o szkoleniach i postępach
 - h) Quizy w języku polskim
 - i) Moduły praktyczne uczące rozpoznawania zagrożeń
 - j) Raportowanie postępów – statusy, wyniki testów, aktywność grup
 - k) Raporty okresowe i końcowe z realizacji szkoleń
 - l) Wsparcie organizacyjne: konfiguracja platformy, zakładanie kont, raportowanie
 - m) Minimum 4 moduły praktyczne rocznie (zamiast 4 kampanii phishingowych)
 - n) Usługa świadczona w chmurze zgodnie ze standardami bezpieczeństwa dostawcy
8. Szkolenia muszą podlegać aktualizacji w przypadku zmian przepisów prawa, norm, wytycznych lub pojawienia się nowych zagrożeń, które mają wpływ na zakres merytoryczny szkolenia. Wykonawca zobowiązuje się do dokonania takiej aktualizacji niezwłocznie, jednak nie częściej niż dwa razy w roku w ramach wynagrodzenia ryczałtowego. Dodatkowo Zamawiający ma prawo zgłosić potrzebę aktualizacji treści szkolenia, jeżeli uzasadniają to zmiany organizacyjne lub technologiczne po stronie Zamawiającego. W takim przypadku Wykonawca dokonuje aktualizacji w ramach wynagrodzenia, o ile dotyczy ona materiału o zakresie nie większym niż 20% objętości szkolenia. W przypadku zgłoszeń wykraczających poza wskazany zakres strony ustalą dodatkowe wynagrodzenie przed rozpoczęciem prac. Aktualizacje, niezależnie od podstawy, obejmują wyłącznie dostosowanie treści merytorycznych bez konieczności tworzenia szkolenia od podstaw.
9. Wykonawca przygotowuje i dostarczy materiały szkoleniowe związane z wdrożeniem oraz stosowaniem udokumentowanego SZBI dla pozostałych pracowników Zamawiającego. Celem materiałów jest zapewnienie pracownikom możliwości szybkiego zapoznania się z wymaganiami wynikającymi z Polityk i Procedur SZBI oraz stosowania ich w codziennej pracy.

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

10. Wykonawca zapewni prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
- a) Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
 - b) Lista odbioru zaświadczeń o ukończeniu szkolenia.

Terminy, zasady i warunki realizacji Przedmiotu Zamówienia

Terminy realizacji prac, odbiór oraz wymagania stawiane Wykonawcy

1. Wykonawca zrealizuje Przedmiot Zamówienia w zakresie i podziale na etapy.
2. Realizacja poszczególnych etapów będzie realizowana w następujących terminach:
 - a) **Etap 1** – do **7 dni** od dnia podpisania Umowy;
 - b) **Etap 2** – do **7 dni** od zakończenia Etapu 1;
 - c) **Etap 3** – do **30 dni** od zakończenia Etapu 2.
3. Każdy z etapów realizacji Przedmiotu Zamówienia, podlega odrębnemu odbiorowi przez Zamawiającego. Odbiór każdego etapu nastąpi na podstawie Protokołu Odbioru Częściowego, sporządzonego przez Strony i podpisanego bez zastrzeżeń.
4. Zamawiający zastrzega sobie prawo do wniesienia uwag do zawartości raportu z przeprowadzonego audytu bezpieczeństwa, do treści dokumentacji SZBI oraz materiałów szkoleniowych, zgłaszanych w trakcie procedury odbiorowej.
5. Po zakończeniu realizacji wszystkich etapów Przedmiotu Zamówienia, Strony podpiszą Protokół Odbioru Końcowego, który będzie stanowił podstawę do wystawienia przez Wykonawcę faktury VAT za wykonanie całości Przedmiotu Zamówienia.
6. System Zarządzania Bezpieczeństwem Informacji musi obejmować wszystkie zasoby informacyjne Szpitala, w tym: systemy medyczne (HIS, LIS, RIS, EDM), systemy administracyjne, serwery, urządzenia sieciowe, stacje robocze, systemy backupowe, infrastrukturę OT/IoMT (urządzenia medyczne podłączone do sieci), dane przetwarzane poza systemami informatycznymi oraz procesy organizacyjne.

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

7. Wykonawca uwzględni w dokumentacji SZBI zmieniającą się infrastrukturę sprzętowo-systemową i zakupywane rozwiązania z zakresu cyberbezpieczeństwa w trakcie realizacji Projektu pn. „Transformacja cyfrowa Szpitala Wielospecjalistycznego w Jaworznie – integracja systemów, digitalizacja dokumentacji i wzrost cyberbezpieczeństwa”.
8. Wszystkie procedury i polityki muszą być opracowane w oparciu o normy ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO 22301; ustawę o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560) z późn. zmianami, zgodnie z rozporządzeniem RODO, Rozporządzeniem KRI oraz wymaganiami KPO – inwestycja D1.1.2, wskaźnik D21G.R2.
9. Wykonawca do realizacji prac skieruje zespół ekspertów składający się z audytorów/specjalistów spełniających warunki udziału w postępowaniu opisane w Zapytaniu Ofertowym.

Warunki realizacji usług szkoleniowych

1. Szkolenia określone jako Etap 3 zostaną zrealizowane w siedzibie Zamawiającego lub w trybie zdalnym za zgodą Zamawiającego.
2. Każdemu uczestnikowi szkoleń Wykonawca wystawi imienny certyfikat uczestnictwa.
3. Szkolenia, które będą przeprowadzone w placówce Zamawiającego muszą być realizowane w dni robocze w godzinach od 7:30 do 14:30.
4. Wykonawca jest zobowiązany przedstawić Zamawiającemu propozycję szczegółowego harmonogramu szkoleń nie później niż na 3 dni robocze przed planowanym rozpoczęciem szkoleń.
5. Wykonawca jest zobowiązany do uwzględnienia uwag przekazanych przez Zamawiającego, a w przypadku braku takiej możliwości, do przedstawienia nowej propozycji harmonogramu szkoleń w terminie maksymalnie 2 dni roboczych od przekazania uwag.
6. Wykonawca przygotuje i dostarczy materiały szkoleniowe związane z wdrożeniem oraz stosowaniem udokumentowanego SZBI dla pozostałych pracowników Zamawiającego. Celem materiałów jest zapewnienie pracownikom możliwości szybkiego zapoznania się z wymaganiami wynikającymi z Polityk i Procedur SZBI oraz stosowania ich w codziennej pracy.
7. Pod pojęciem „materiałów szkoleniowych” Zamawiający rozumie w szczególności:
 - prezentacje szkoleniowe (PPT/PDF) dotyczące zasad SZBI i obowiązków pracowników,
 - skrócone instrukcje / karty pracownika („one-pagery”) z kluczowymi zasadami bezpieczeństwa i zgłaszania incydentów,
 - checklisty dotyczące bezpiecznej pracy z systemami i danymi, – dokument podsumowujący SZBI dla pracowników.

Samodzielny Publiczny Zakład Opieki Zdrowotnej Szpital Wielospecjalistyczny w Jaworznie; 43-600 Jaworzno; ul. Chełmońskiego 28,
NIP: 632-17-53-077, REGON 270641184, tel. 32 317 45 11

Materiały mają umożliwić pracownikom szybkie zapoznanie się z zasadami SZBI i ich stosowanie w codziennej pracy.

8. Materiały szkoleniowe muszą być przygotowane w języku polskim, w formie elektronicznej, edytowalnej oraz w formie PDF.

Wsparcie wdrożenia ze strony Zamawiającego

1. Zamawiający umożliwi Wykonawcy prawidłowe wykonanie Przedmiotu Zamówienia, poprzez:
 - a) Udostępnienie lokalizacji na czas niezbędny do wykonania Przedmiotu Zamówienia.
 - b) Dostęp do wszelkich informacji i środków technicznych niezbędnych do realizacji Przedmiotu Zamówienia. Dostęp do informacji oznacza udostępnianie w postaci dokumentów papierowych lub elektronicznych dokumentacji i innych opracowań oraz informacji uzyskanych od pracowników Zamawiającego, które na podstawie uzasadnionego wniosku Wykonawcy mogą mieć wpływ na realizację Przedmiotu Zamówienia.
 - c) Zamawiający wyznaczy pracownika odpowiedzialnego za współpracę z Wykonawcą oraz nadzór nad wdrożeniem.
2. W szczególności Zamawiający zobowiązuje się do:
 - a) Współpracy z Wykonawcą na każdym etapie realizacji Przedmiotu Zamówienia;
 - b) Udzielenia dostępu do dokumentacji i topologii infrastruktury sieciowej;
 - c) Udzielenia dostępu do raportów z dotychczas przeprowadzonych audytów;
 - d) Udzielenia dostępu do pełnomocników/koordynatorów ds. bezpieczeństwa, inspektora ochrony danych oraz administratorów systemów IT;
 - e) Użyczenie pomieszczenia w siedzibie Zamawiającego w celu prowadzenia szkoleń i badań audytowych przez zespół audytowy Wykonawcy.