

Załącznik nr 3 do SWZ

Dotyczy postępowania: ZP/22/2026

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest:

- a. Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w celu osiągnięcia zgodności z wymogami NIS2, w tym niezbędne szkolenia dla personelu z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny);
- b. Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w zakresie ciągłości działania, obejmującej analizę wpływu na biznes, opracowanie strategii oraz scenariuszy postępowania, w tym przeszkolenie personelu związane wdrożeniem oraz stosowaniem udokumentowanego SZBI oraz przeprowadzenie Audytu końcowego w obszarze cyberbezpieczeństwa, w tym w zakresie spełnienia przez Szpital wymagań określonych w Ankiecie weryfikacji dojrzałości pod kątem cyberbezpieczeństwa, stanowiącej element Załącznika nr 4 – Zakres realizacji przedsięwzięcia do wyboru przedsięwzięcia do REGULAMINU WYBORU PRZEDSIĘWZIĘCIA DO OBJĘCIA WSPARCIEM W RAMACH KRAJOWEGO PLANU ODBUDOWY I ZWIĘKSZANIA ODPORNOŚCI Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia” Nabór nr KPOD.07.03-IP.10-001/25 (tryb konkurencyjny – I nabór – Inwestycja D.1.1.2)

Przedmiot zamówienia obejmuje opracowanie oraz wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), przeprowadzenie szkolenia dla personelu z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny) dla kadry szpitala, przeszkolenie personelu związane wdrożeniem oraz stosowaniem udokumentowanego SZBI, przeprowadzenie końcowego audytu wraz z Ankietą weryfikacji dojrzałości pod kątem cyberbezpieczeństwa. Zamawiający funkcjonuje jako Operator Usługi Kluczowej (OUK) i wchodzi w skład Krajowego Systemu Cyberbezpieczeństwa (KSC) w związku z czym wymagana jest realizacja usług z uwzględnieniem wskazanego statusu Zmawiającego.

Zamawiający wymaga opracowania dokumentacji i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) uwzględniającego kontekst organizacyjny Zamawiającego wraz z przekazaniem praw autorskich do SZBI, w celu osiągnięcia zgodności funkcjonowania Szpitala z wymogami:

- a. DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)
- b. normy PN-EN ISO/IEC 27001, ISO/IEC 27002 i ISO/IEC 27005 oraz ISO 22301,
- c. ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307),
- d. przepisami rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI),

- e. wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), z uwzględnieniem jej aktualnych oraz potencjalnych zmian legislacyjnych w okresie realizacji zamówienia,
- f. przepisów ustawy o ochronie danych osobowych i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
- g. innych powszechnie uznanych i stosowanych dobrych praktyk i regulacji w przedmiotowym zakresie

w zakresie obejmującym co najmniej procesy i usługi świadczone przez Zamawiającego.

Przedmiot zamówienia jest współfinansowany przez Unię Europejską z Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”, będącej elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia” i musi zostać zrealizowany zgodnie z wymaganiami określonymi w REGULAMINIE WYBORU PRZEDSIĘWZIĘCIA DO OBJĘCIA WSPARCIEM W RAMACH KRAJOWEGO PLANU ODBUDOWY I ZWIĘKSZANIA ODPORNOŚCI Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia” Nabór nr KPOD.07.03-IP.10-001/25 dostępnym pod adresem: <https://www.gov.pl/web/zdrowie/inwestycja-d112-przyspieszenie-procesow-transformacji-cyfrowej-ochrony-zdrowia-poprzez-dalszy-rozwoj-uslug-cyfrowych-w-ochronie-zdrowia-nabor-konkurencyjny> - w wersji obowiązującej na dzień zawarcia umowy oraz wytycznymi Ministerstwa Zdrowia oraz rekomendacjami Centrum e-Zdrowia.

Celem realizacji zamówienia jest uzyskanie kompleksowej wiedzy na temat poziomu zgodności szpitala z wymaganiami norm ISO/IEC 27001 oraz ISO 22301, w tym identyfikacja luk oraz obszarów ryzyka w zakresie cyberbezpieczeństwa i ciągłości działania, a także przygotowanie organizacji do wdrożenia, utrzymania oraz ewentualnej certyfikacji systemów zarządzania. Realizacja prac ma przyczynić się do zwiększenia poziomu bezpieczeństwa informacji – w szczególności danych medycznych i danych osobowych pacjentów – oraz zapewnienia ciągłości działania kluczowych procesów szpitalnych, w tym nieprzerwanej opieki nad pacjentami.

Zakres prac obejmuje w szczególności przegląd istniejącej dokumentacji i procedur w obszarze bezpieczeństwa informacji oraz ciągłości działania, ocenę zgodności stosowanych rozwiązań z wymaganiami norm ISO/IEC 27001:2022 oraz ISO 22301:2019, analizę zabezpieczeń organizacyjnych, technicznych i fizycznych, weryfikację przypisania ról i odpowiedzialności, a także ocenę ryzyk oraz adekwatności wdrożonych środków kontrolnych. Efektem realizacji zamówienia będzie przygotowanie raportu zawierającego wnioski i rekomendacje, stanowiącego dokumentację wynikową z przeprowadzonych prac.

Zamawiający wymaga aby opracowanie i wdrożenie kompletnego SZBI było poprzedzone kompleksową analizą stanu faktycznego jednostki Zamawiającego co najmniej w zakresie:

- diagnozy przedwdrożeniowej wykonanej w siedzibie jednostki Zamawiającego;
- analizy dokumentacji jednostki i zapoznania się z dostępnymi regulacjami wewnętrznymi mającymi wpływ na bezpieczeństwo informacji, identyfikacji istniejących rozwiązań organizacyjnych i technicznych;
- przeprowadzenia przez Wykonawcę analizy w organizacji, w tym co najmniej:
 - a. wywiady z kluczowymi pracownikami, pełniącymi funkcje istotne z perspektywy bezpieczeństwa informacji ,
 - b. weryfikacja zgodności aktualnej dokumentacji i procedur z wymogami jakim musi odpowiadać jednostka Zamawiającego uwzględniając jej status jako Operator Usługi Kluczowej, w tym ocenę ich zgodności z wymaganiami norm ISO/IEC 27001 oraz ISO 22301,,
 - c. identyfikacja i analiza luk w organizacji pod kątem zapewnienia bezpieczeństwa informacji oraz spełniania wymagań normy ISO 27001.
 - d. ocena poziomu dojrzałości organizacji w zakresie:

- zarządzania bezpieczeństwem informacji,
- zarządzania ciągłością działania.

Raport i rekomendacje

Efektom realizacji analizy stanu będzie opracowanie raportu zawierającego:

- podsumowanie wyników przeprowadzonej analizy,
- wykaz stwierdzonych niezgodności oraz ich klasyfikację (np. krytyczne, istotne, drobne),
- ocenę poziomu dojrzałości organizacji,
- szczegółowe rekomendacje działań naprawczych i doskonalących,
- propozycję harmonogramu wdrożenia działań dostosowawczych,
- wskazanie priorytetów działań z punktu widzenia bezpieczeństwa pacjentów oraz ciągłości świadczenia usług medycznych.

1. Zakres zamówienia dotyczący kompletnej dokumentacji SZBI

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do opracowania kompletnej dokumentacji SZBI obejmującej co najmniej następujące obszary:

a) Dokumenty nadrzędne i systemowe:

- Polityka bezpieczeństwa informacji (cyberbezpieczeństwa),
- Polityka ciągłości działania (BCP/DRP),
- Metodyka zarządzania ryzykiem wraz z rejestrem ryzyk.

b) Obszary organizacyjne i operacyjne

- zarządzanie incydentami cyberbezpieczeństwa,
- zarządzanie aktywami informacyjnymi,
- zarządzanie bezpieczeństwem fizycznym,
- zarządzanie bezpieczeństwem osobowym,
- zarządzanie bezpieczeństwem środowiskowym.

c) Obszary techniczne

- zarządzanie bezpieczeństwem sprzętu,
- zarządzanie nośnikami danych,
- zarządzanie urządzeniami mobilnymi,
- zarządzanie tożsamością i dostępem (IAM),
- zarządzanie bezpieczeństwem sieci i systemów,
- zarządzanie bezpieczeństwem komunikacji.

d) Obszary wsparcia i rozwoju

- program szkoleń i podnoszenia świadomości pracowników (w tym cyberhigiena),
- stosowanie zabezpieczeń kryptograficznych,
- bezpieczeństwo prac rozwojowych (Secure SDLC),
- zarządzanie relacjami z dostawcami i wykonawcami.

e) Cykl życia systemów i podatności

- bezpieczeństwo w procesie nabywania, rozwoju i utrzymania systemów IT,
- zarządzanie podatnościami technicznymi i aktualizacjami.

f) Monitorowanie, audyt i zgodność

- monitorowanie i pomiary skuteczności zabezpieczeń,
- audyty wewnętrzne cyberbezpieczeństwa,
- zarządzanie zgodnością z przepisami prawa, normami i umowami.

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w zakresie ciągłości działania, obejmującej analizę wpływu na biznes, opracowanie strategii oraz scenariuszy postępowania:

W ramach zamówienia Wykonawca zobowiązany jest do:

- a) opracowania i/lub aktualizacji dokumentacji Systemu Zarządzania Ciągłością Działania zgodnie z wymaganiami normy ISO 22301, w tym:
 - polityki ciągłości działania,
 - planów ciągłości działania (BCP),
 - planów odtwarzania po awarii (DRP),
- b) identyfikacji procesów krytycznych dla funkcjonowania szpitala, w szczególności:
 - procesów związanych z udzielaniem świadczeń zdrowotnych,
 - procesów diagnostycznych i laboratoryjnych,
 - funkcjonowania systemów IT wspierających opiekę nad pacjentem,
- c) przeprowadzenia analizy wpływu na działalność (Business Impact Analysis – BIA),
- d) określenia parametrów ciągłości działania (RTO, RPO),
- e) identyfikacji zagrożeń dla ciągłości działania oraz opracowania scenariuszy awaryjnych,
- f) oceny gotowości organizacji do reagowania na sytuacje kryzysowe.

Zakres prac w obszarze ciągłości działania (ISO 22301)

Przedmiotem zamówienia jest opracowanie, uzgodnienie oraz przygotowanie do wdrożenia kompletnej dokumentacji systemu zarządzania ciągłością działania (BCMS – Business Continuity Management System) zgodnej z wymaganiami normy ISO 22301, z uwzględnieniem specyfiki działalności Zamawiającego (podmiot leczniczy) oraz obowiązujących przepisów prawa, w tym ustawy o krajowym systemie cyberbezpieczeństwa oraz wytycznych NIS2.

Zakres prac obejmuje w szczególności:

- a) Etap przygotowawczy i inicjujący
 - identyfikację interesariuszy wewnętrznych i zewnętrznych,
 - określenie zakresu systemu zarządzania ciągłością działania (BCMS).
- b) Identyfikacja procesów i zasobów
 - identyfikację i mapowanie kluczowych procesów biznesowych, w tym procesów medycznych i wspierających,
 - identyfikację zasobów krytycznych (ludzkich, technicznych, infrastrukturalnych, informacyjnych),
 - określenie zależności pomiędzy procesami oraz zasobami.
- c) Analiza wpływu na biznes (BIA)
 - przeprowadzenie analizy wpływu na biznes (Business Impact Analysis), obejmującej:
 - określenie maksymalnych dopuszczalnych czasów przerwy (MTPD),
 - określenie docelowych czasów odtworzenia (RTO) oraz poziomów odtworzenia danych (RPO),
 - analizę skutków zakłóceń dla działalności operacyjnej, finansowej, prawnej i reputacyjnej,
 - klasyfikację procesów według krytyczności.
- d) Analiza ryzyka
 - identyfikację zagrożeń dla ciągłości działania (w tym cyberzagrożeń),
 - analizę podatności i ocenę ryzyka dla zidentyfikowanych procesów i zasobów,
 - określenie poziomu akceptowalnego ryzyka,
 - wskazanie działań minimalizujących ryzyko.
- e) Opracowanie strategii ciągłości działania
 - opracowanie strategii zapewnienia ciągłości działania dla kluczowych procesów,
 - określenie rozwiązań organizacyjnych i technicznych zapewniających odtwarzanie działalności,
 - uwzględnienie scenariuszy awaryjnych, w tym:
 - awarii systemów IT,
 - utraty infrastruktury,

- niedostępności personelu,
 - incydentów cyberbezpieczeństwa.
- f) Opracowanie dokumentacji BCMS, obejmującą co najmniej:
- Politykę ciągłości działania,
 - metodykę zarządzania ciągłością działania,
 - procedurę zarządzania incydentami i sytuacjami kryzysowymi,
 - plany ciągłości działania (BCP),
 - plany odtworzeniowe (DRP – Disaster Recovery Plans),
 - procedury awaryjne dla kluczowych procesów,
 - plan komunikacji kryzysowej,
 - matrycę ról i odpowiedzialności (np. RACI),
 - scenariusze testów i ćwiczeń.
- g) Konsultacje i uzgodnienia
- bieżące konsultacje z Zamawiającym na każdym etapie realizacji,
 - przeprowadzenie warsztatów uzgodnieniowych,
 - dostosowanie dokumentacji do struktury organizacyjnej i specyfiki szpitala.
- h) Przekazanie dokumentacji
- przekazanie kompletnej dokumentacji: w wersji elektronicznej (edytowalnej i PDF), i w wersji papierowej,
 - zapewnienie spójności dokumentacji z wymaganiami ISO 22301 oraz powiązania z dokumentacją SZBI (ISO 27001).

2. Zakres zamówienia dotyczący szkoleń

W ramach zamówienia Wykonawca zobowiązany będzie do:

- opracowania programu szkoleń z zakresu podnoszenia świadomości cyberbezpieczeństwa (cyberhigieny), oraz wdrożenia oraz stosowania udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji,
- przeprowadzenia szkoleń personelu związanych z wdrożeniem oraz stosowaniem udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji;
- przeprowadzenia szkoleń dla kadry kierowniczej oraz personelu Zamawiającego w zakresie podnoszenia świadomości cyberbezpieczeństwa (cyberhigieny),
- przekazania materiałów szkoleniowych umożliwiających dalsze prowadzenie działań edukacyjnych wewnątrz organizacji.

Minimalny zakres szkoleń z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny):

Szkolenia kadry kierowniczej, co najmniej z:

- Podstaw prawnych w obszarze cyberbezpieczeństwa.
- Typów ataków wraz z przykładami
- Reagowania na incydenty.
- Wykonywania testów bezpieczeństwa.
- Roli kadry zarządzającej w procesach bezpieczeństwa.

Szkolenia pracowników administracji i pracowników medycznych, co najmniej z:

- Podstawowych zasad cyberhigieny.
- Typów ataków wraz z przykładami
- Reagowania na incydenty

Odpowiedzialności prawnej

Minimalny zakres szkoleń z zakresu SZBI:

- stosowanie opracowanych procedur,

- reagowanie na sytuacje kryzysowe,
- zasad ciągłości działania,
- omówienie zasad prawidłowego postępowania w zakresie cyberbezpieczeństwa obowiązujących w Szpitalu,
- przedstawienie aktualnych zagrożeń w cyberprzestrzeni, w tym w szczególności: phishing, ransomware, malware, socjotechnika, ataki telefoniczne, spoofing, ataki typu „odwrócony phishing”, oszustwa typu „na prezesa/dyrektora”, wyłudzenia BLIK oraz tzw. „przekręty nigeryjskie” – wraz z przykładami oraz metodami zapobiegania i reagowania,
- wyjaśnienie podstawowych pojęć, w tym istoty cyberbezpieczeństwa,
- omówienie metod nieautoryzowanego pozyskiwania danych wraz z przykładami,
- przedstawienie zasad bezpiecznego przetwarzania danych, w tym szyfrowania, przechowywania, udostępniania oraz bezpiecznej komunikacji,
- zaprezentowanie metod ochrony i przeciwdziałania zagrożeniom, w szczególności w zakresie ochrony przed wyłudzeniami danych, atakami socjotechnicznymi, złośliwym oprogramowaniem oraz incydentami skutkującymi utratą dostępu do systemów,
- omówienie zasad bezpiecznego korzystania z mediów społecznościowych oraz urządzeń mobilnych, w tym smartfonów,
- wskazanie kluczowych zasobów, informacji i obszarów wymagających szczególnej ochrony w celu ograniczenia ryzyka strat,
- przedstawienie zasad cyberhigieny i dobrych praktyk bezpieczeństwa.

Liczba osób do przeszkolenia: 392 personelu Zamawiającego.

Forma poświadczenia udziału w szkoleniu: uzyskanie od uczestników szkoleń oświadczeń potwierdzających udział w formie podpisanych list obecności.

Forma materiałów szkoleniowych: papierowa oraz elektroniczna – dostarczenie przed rozpoczęciem szkoleń.

Po zakończeniu szkoleń – przekazanie nagrań ze szkoleń.

Stworzenie możliwości udziału w szkoleniach stacjonarnie w siedzibie Zamawiającego oraz on-line.

3. Zakres zamówienia dotyczący audytu końcowego w obszarze cyberbezpieczeństwa

Audyt powinien obejmować przynajmniej obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych (aparatura medyczna wraz z systemami je obsługującymi). Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:

- Kanały komunikacji jak np. poczta
- Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów
- Kontrolery domeny
- Platforma wirtualizacyjna
- System zarządzania kopiami zapasowymi
- Poprawność konfiguracji stacji roboczych oraz serwerów
- Sposoby uwierzytelniania się użytkowników

Rezultaty zamówienia:

Wykonanie zamówienia musi pozwolić na spełnienie wymagań określonych poniżej jako obligatoryjne:

System zarządzania bezpieczeństwem informacji

| Lp. | Nazwa kryterium | Czy obligatoryjne? |
|-----|---|--------------------|
| 1. | Wdrożono politykę zarządzania dostępem i uprawnieniami. | Tak |
| 2. | Wdrożono politykę kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania. | Tak |
| 3. | Wdrożono politykę zarządzania podatnościami | Tak |
| 4. | Wdrożono politykę zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa | Tak |
| 5. | Wdrożono politykę logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny. | Tak |
| 6. | Wdrożono politykę kopii bezpieczeństwa. | Tak |
| 7. | Wdrożono politykę zarządzania incydentami bezpieczeństwa. | Tak |
| 8. | Wdrożono politykę zarządzania ciągłością działania. | Tak |
| 9. | Wdrożono politykę ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych | Tak |

Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

| Lp. | Nazwa kryterium | Czy obligatoryjne? |
|-----|---|--------------------|
| 1. | Odbycie szkolenia przez kadrę kierowniczą, w okresie ostatniego roku, minimum w zakresie: <ul style="list-style-type: none"> Podstaw prawnych w obszarze cyberbezpieczeństwa Typów ataków Reagowania na incydenty Wykonywania badań bezpieczeństwa Roli kadry zarządzającej w procesach bezpieczeństwa | Tak |
| 2. | Odbycie szkolenia przez kadrę biurową i medyczną – min. 75% pracowników pracujących na systemach informatycznych szpitala, w okresie ostatniego roku, minimum w zakresie: <ul style="list-style-type: none"> Podstawowych zasad cyberhigieny Typów ataków wraz z przykładami Reagowania na incydenty | Tak |

Wymagania dotyczące zespołu projektowego

Zespół audytujący: co najmniej dwóch audytorów posiadających certyfikaty określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu lub co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub jednostka oceniająca zgodność, akredytowana zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 z późn.zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych.