

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup usługi aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

i Systemu Zarządzania Ciągłością Działania

Przedmiotem zamówienia jest zakup usługi aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i Systemu Zarządzania Ciągłością Działania Szpitala w ramach projektu Rozwój usług cyfrowych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej Wojewódzkim Szpitalu Specjalistycznym nr 3 w Rybniku w ramach KPO na lata 2021-2026 DZIAŁANIE 1.1.2 „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”.

1. Szczegółowy opis przedmiotu zamówienia:

1) Opracowanie dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z wymaganiami:

- i 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,
- ii ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa z późn. zm.,
- iii rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- iv wg wymagań normy ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301 wraz z wdrożeniem.

2) Wykonawca zobowiązany jest do wytworzenia dokumentacji, formularzy, opracowania zasad postępowania, procedur itd., zgodnie z wymaganiami opisanymi w dalszej części niniejszego dokumentu

3) Etap I – Powołanie zespołu i ustalenie zasad współpracy:

- i) prawne aspekty wdrożenia SZBI,
- ii) powołanie zespołu SZBI,
- iii) omówienie celów, ról, harmonogramu prac, zasad komunikacji,
- iv) ustalenie sposobu przekazywania danych, potwierdzania i zatwierdzania etapów.

4) Etap II - Identyfikacja informacji i zasobów:

- i) zapoznanie się ze strukturą organizacyjną JST,
- ii) analiza Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i Systemu Zarządzania Ciągłością Działania szpitala,
- iii) inwentaryzacja informacji,
- iv) wycena informacji w kategoriach: poufność / dostępność / integralność.
- v) inwentaryzacja zasobów,
- vi) mapowanie informacji do zasobów.

5) Etap III – Ocena ryzyka:

- i) identyfikacja zagrożeń i podatności,
- ii) ocena prawdopodobieństwa i skutków wystąpienia ryzyk,
- iii) ustalenie poziomu akceptowalnego ryzyka,
- iv) opracowanie planu postępowania z ryzykiem we współpracy z ASI oraz kadrą zarządzającą podmiotu.

6) Etap IV – Opracowanie dokumentacji SZBI. Zakres dokumentacji:

- i) polityka bezpieczeństwa informacji (dokument nadrzędny),
- ii) polityka zarządzania dostępem i uprawnieniami,
- iii) polityka kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania,
- iv) polityka zarządzania podatnościami
- v) polityka zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa

vi polityka logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brze-
gowej, kontrolerem domeny.

vii polityka kopii bezpieczeństwa.

viii polityka zarządzania incydentami bezpieczeństwa.

ix polityka zarządzania ciągłością działania.

x polityka ochrony danych osobowych z uwzględnieniem przetwarzania danych me-
dycznych

xi polityka zarządzania ryzykiem urządzeń bez rozwiązania EDR

xii procedury operacyjne (nadawanie uprawnień, kopie zapasowe, incydenty, klasyfika-
cja informacji),

xiii instrukcje i wzory dokumentów (np. oświadczenia, polityka haseł, matryca dostę-
pu),

xiv dokumentacja wynikowa z analizy ryzyka i planów działań.

xv Przekazanie kompletnej dokumentacji SZBI – podsumowanie etapu.

7) Etap V – Wdrożenie procedur SZBI:

i wydanie zarządzenia o wdrożeniu SZBI,

ii podział na grupy, których dotyczy dana dokumentacja i procedury dotyczą,

iii szkolenie kierownictwa i pracowników z zasad bezpieczeństwa informacji,

iv wprowadzenie dokumentacji do stosowania (procedury, rejestry),

v zakończenie prac wdrożeniowych.

8) Etap VI – Przegląd po przygotowaniu i wdrożeniu SZBI:

i monitorowanie, przeglądy, ocena,

ii poprawki, aktualizacja,

iii monitorowanie postępu wdrożonych procedur oraz weryfikacja stosowania,

iv przygotowanie planu minimalizujący ryzyko po wdrożeniu SZBI przez okres 1 roku

2. Organizacja realizacji przedmiotu zamówienia:

1) Etap III i V - w siedzibie Zamawiającego

2) Etap I, II, IV, VI - z wykorzystaniem zdalnej komunikacji.

3) Potwierdzeniem wykonania prac będzie odbiór wszystkich etapów prac tego zadania.

4) Wszystkie dokumenty sporządzone będą w formie pisemnej w języku polskim w formacie pdf oraz w formacie edytowalnym.

5) Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty niniejszego zamówienia.

Termin realizacji zadania - do dnia 26.06.2026 r.

..... dnia

(miejscowość)

.....

(podpis(y) osoby (osób) upoważnionej
do występowania w imieniu Wykonawcy