Załącznik nr 2 do zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

Informacje ogólne: Przedmiotem zamówienia jest opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Zamawiający wchodzi w skład Krajowego Systemu Cyberbezpieczeństwa (KSC) w związku z czym wymagana jest realizacja usług z uwzględnieniem wskazanego statusu Zamawiającego - podmiot kluczowy.

Usługi Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) Zamawiający wymaga opracowania i wdrożenia dokumentacji 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:

1. ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), z uwzględnieniem jej aktualnych oraz potencjalnych zmian legislacyjnych w okresie realizacji zamówienia,
2. Polskiej Normy PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-10 i ISO/IEC 27005,
3. rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI),
4. ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307),
5. przepisów ustawy o ochronie danych osobowych i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
6. ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (w zakresie tajemnicy informacji z nim związanych),
7. Ministerstwa Zdrowia oraz rekomendacji Centrum e-Zdrowia, w ramach którego realizowany jest przedmiot zamówienia,
8. innych powszechnie uznanych i stosowanych dobrych praktyk i regulacji w przedmiotowym zakresie.

Celem realizacji zamówienia jest uzyskanie kompleksowej wiedzy na temat poziomu zgodności szpitala z wymaganiami norm PN-EN ISO/IEC 27001:2023-08, 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 PN-EN ISO/IEC 27001:2023-08, analizę zabezpieczeń organizacyjnych, technicznych i fizycznych, weryfikację przypisania ról i odpowiedzialności (w tym struktur

kontaktowych wymaganych przez KSC), 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 dokumentacji kompletnego SZBI było poprzedzone kompleksową analizą stanu faktycznego jednostki Zamawiającego co najmniej w zakresie:

1. Diagnozy przedwdrożeniowej wykonanej w siedzibie jednostki Zamawiającego.
2. Analizy dokumentacji jednostki i zapoznania się z dostępnymi regulacjami wewnętrznymi mającymi wpływ na bezpieczeństwo informacji.
3. Przeprowadzenia przez Wykonawcę audytu w organizacji, w tym co najmniej:
    1) wywiady z kluczowymi pracownikami, pełniącymi funkcje istotne z perspektywy bezpieczeństwa informacji,
    2) weryfikacja zgodności aktualnej dokumentacji i procedur z wymogami jakim musi odpowiadać jednostka Zamawiającego,
    3) identyfikacja i analiza luk w organizacji pod kątem zapewnienia bezpieczeństwa informacji oraz spełniania wymagań normy PN-EN ISO/IEC 27001:2023-08.
4. Opracowania wyników audytu.
5. Opracowania raportu wraz z propozycją planu realizacji SZBI.

Zamawiający wymaga aby opracowanie i wdrożenie kompletnego SZBI było skorelowane z procesem przeprowadzenia Analizy Ryzyka, który również Wykonawca musi przeprowadzić co najmniej w zakresie:

1. Przedstawienia propozycji metodyki analizy ryzyka w ramach Systemu Zarządzania Bezpieczeństwem Informacji, uwzględniającej specyfikę ryzyk dla systemów informacyjnych, w których przetwarzane są usługi kluczowe (zgodnie z KSC).
2. Przeprowadzenia inwentaryzacji aktywów związanych z przetwarzaniem informacji oraz ich klasyfikacji uwzględniając specyfikę jednostki organizacyjnej Zamawiającego.
3. Opracowania Planu Postępowania z Ryzykiem (RTP - Risk Treatment Plan) określającego sposoby mitygacji zidentyfikowanych zagrożeń.
4. Opracowania raportu zbiorczego obejmującego co najmniej podsumowanie zrealizowanych prac i wynikających z tego wniosków.

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji musi zawierać co najmniej:

L.p.	Nazwa dokumentu / polityki	Czy obligatoryjna?
1	Nadrzędna Polityka Bezpieczeństwa Informacji (deklaracja intencji i celów kierownictwa, zgodnie z wymaganiami HLS ISO 27001)	Tak
2	Deklaracja Stosowania (SoA - Statement of Applicability) uzasadniająca wybór zabezpieczeń z Załącznika A normy ISO 27001	Tak
3	Polityka / Procedura zarządzania dostępem i uprawnieniami	Tak
4	Polityka kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania	Tak

5	Polityka / Procedura zarządzania podatnościami	Tak
6	Polityka / Metodyka zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa	Tak
7	Polityka logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolera domeny	Tak
8	Polityka kopii bezpieczeństwa	Tak
9	Polityka / Procedura zarządzania incydentami bezpieczeństwa (wraz z procedurami eskalacji, klasyfikacją incydentów KSC i ścieżkami raportowania do właściwego CSIRT)	Tak
10	Polityka / Procedura zarządzania ciągłością działania (w tym przeprowadzenie Analizy Wpływu na Biznes - BIA dla kluczowych procesów medycznych i administracyjnych)	Tak
11	Metodyka klasyfikacji informacji i postępowania z aktywami informacyjnymi	Tak
12	Procedura przeprowadzania audytów wewnętrznych SZBI	Tak
13	Procedura przeglądu zarządzania SZBI (Management Review)	Tak
14	Procedura zarządzania niezgodnościami i działaniami korygującymi	Tak
15	Polityka zarządzania bezpieczeństwem w relacjach z dostawcami (z uwzględnieniem dostawców IT, systemów HIS oraz serwisu aparatury medycznej)	Tak
16	Polityka / Procedura budowania świadomości i szkoleń z zakresu cyberbezpieczeństwa dla personelu	Tak
17	Polityka ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych	Tak

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami oraz wszelkich innych informacji uzyskanych w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji, a także wymogów strukturalnych wytycznych normy ISO 27001 w tzw. strukturze wysokiego poziomu (HLS).