OPIS PRZEDMIOTU ZAMÓWIENIA

„Opracowanie, wdrożenie i utrzymanie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)”

Zamawiający:

SP ZOZ w Międzyrzecu Podlaskim

Przedmiotem zamówienia jest opracowanie, wdrożenie i utrzymanie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnej z obowiązującymi regulacjami prawnymi, w tym Dyrektywą NIS2 oraz dobrymi praktykami i normami w zakresie bezpieczeństwa informacji, obejmującej w szczególności polityki, procedury, instrukcje oraz plany reagowania na incydenty, a także **przeprowadzenie audytu bezpieczeństwa**.

Dokumentacja SZBI (wdrożenie dokumentacji, wdrożenie SZBI)

Przedmiotem zamówienia jest kompleksowa realizacja usług w zakresie cyberbezpieczeństwa, obejmująca wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Celem zamówienia jest zaprojektowanie, udokumentowanie i wsparcie wdrożenia w strukturach Zamawiającego spójnego i funkcjonalnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). System ten ma na celu zapewnienie poufności, integralności i dostępności informacji, a także osiągnięcie i utrzymanie zgodności z kluczowymi regulacjami prawnymi i normami.
Kluczowe podstawy normatywne i prawne:
Opracowany i wdrożony SZBI musi być w pełni zgodny z wymaganiami następujących dokumentów (w ich najnowszych, obowiązujących na dzień udzielenia zamówienia wersjach):

a) Norma ISO/IEC 27001 - "Information security, cybersecurity and privacy protection — Information security management systems — Requirements".
b) Norma ISO/IEC 27005 - "Information security, cybersecurity and privacy protection — Guidance on managing information security risks".
c) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
d) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI).
e) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (Dyrektywa NIS 2).

Szczegółowy Zakres Prac
Realizacja zamówienia została podzielona na cztery logiczne, następujące po sobie etapy. Odbiór każdego etapu jest warunkiem koniecznym do rozpoczęcia kolejnego.

ETAP I: Audyt Zerowy i Analiza Luk

1. Przeprowadzenie diagnozy przedwdrożeniowej
2. Analiza dostępnej dokumentacji wewnętrznej Zamawiającego (regulaminy, procedury, instrukcje) pod kątem ich wpływu na bezpieczeństwo informacji.
3. Przeprowadzenie wywiadów z kluczowym personelem (kadra zarządzająca, pracownicy IT, pracownicy medyczni i administracyjni) w celu zmapowania kluczowych procesów przetwarzania informacji.
4. Weryfikacja i identyfikacja luk w istniejących zabezpieczeniach (organizacyjnych, technicznych i fizycznych)
5. Produkt: Opracowanie i przekazanie Zamawiającemu "Raportu z Audytu Zerowego"

ETAP II: Szacowanie i Analiza Ryzyka

1. Opracowanie i przedstawienie do akceptacji Zamawiającego metodyki analizy ryzyka,

2. Wspólna z personelem Zamawiającego identyfikacja i inwentaryzacja aktywów informacyjnych (dane, oprogramowanie, infrastruktura, ludzie).
3. Klasyfikacja zidentyfikowanych aktywów pod względem ich krytyczności (poufność, integralność, dostępność).
4. Przeprowadzenie warsztatów szacowania ryzyka z udziałem właścicieli procesów po stronie Zamawiającego, mających na celu identyfikację zagrożeń, podatności oraz ocenę poziomu ryzyka.
5. Produkt: Opracowanie i przekazanie Zamawiającemu kompletnej dokumentacji z analizy ryzyka,

ETAP III: Opracowanie Dokumentacji Systemowej SZBI

1. Na podstawie wyników Etapu I i II, Wykonawca opracuje kompletny zestaw dokumentacji SZBI.
2. Kluczowy wymóg: Wszystkie dokumenty muszą być opracowane w ścisłej współpracy z Zamawiającym i w pełni dostosowane do specyfiki jego działalności, procesów (medycznych i administracyjnych), zasobów oraz infrastruktury.
3. Minimalny zakres dokumentacji:
    - Księga SZBI (podręcznik systemu).
    - Polityka Bezpieczeństwa Informacji.
    - Deklaracja Stosowania (SoA).
    - Polityka kryptografii
    - Polityka Ochrony Danych Osobowych (zgodna z RODO).
    - Polityki szczegółowe, zasady i procedury obejmujące m.in.:
        - Zarządzanie aktywami.
        - Bezpieczeństwo osobowe (cykl życia pracownika).
        - Zarządzanie uprawnieniami i dostępem.
        - Bezpieczeństwo fizyczne i środowiskowe.
        - Bezpieczeństwo teleinformatyczne (sieci, systemy, aplikacje).
        - Zarządzanie incydentami bezpieczeństwa informacji.
        - Zarządzanie ciągłością działania.
        - Zasady zgodności z wymaganiami prawnymi i umownymi.
    - Polityki i szczegółowe zasady i procedury winny również uwzględnić takie dokumenty jak:
        - Polityka klasyfikacji informacji,
        - Polityka zarządzania dostępem i uprawnieniami,
        - Polityka zarządzania podatnościami,
        - Polityka zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa i przetwarzania danych osobowych,
        - Polityka zarządzania incydentami cyberbezpieczeństwa i danych osobowych,
        - Polityka zarządzania ciągłością działania z uwzględnieniem Planu Ciągłości Działania (BCP) oraz Plan Odzyskiwania po Awarii (DisasterRecovery Plan - DRP),
        - Polityka logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolera domeny,
        - Procedura zarządzania dostawcami (zarządzania łańcuchem dostaw),

        - Procedura zarządzania zmianami w urządzeniach i systemach IT,
        - Procedura zarzadzania pojemnością i wydajnością krytycznych zasobów teleinformatycznych,
        - Procedura zarządzania dokumentacja i zapisami SZBI,
        - Procedura audytów wewnętrznych SZBI.
    - Inne dokumenty (instrukcje, regulaminy, wzory oświadczeń), których potrzeba opracowania zostanie zidentyfikowana i uzasadniona na podstawie wyników Etapu I i II,
4. Produkt: Kompletna, zatwierdzona przez Zamawiającego dokumentacja SZBI w edytowalnej formie elektronicznej (np. format .docx).

ETAP IV: Wsparcie Wdrożeniowe i Transfer Wiedzy

1. Przygotowanie dedykowanych materiałów szkoleniowych z SZBI
2. Wsparcie konsultacyjne i merytoryczne dla zespołu Zamawiającego przy przeprowadzeniu pierwszego audytu wewnętrznego SZBI.
3. Aktywne wsparcie konsultacyjne i merytoryczne przy organizacji i przeprowadzeniu pierwszego przeglądu zarządzania SZBI.
4. Produkt:
    - Materiały szkoleniowe w formie elektronicznej.
    - Protokół/raport z przeprowadzonych szkoleń (zawierający program i listę uczestników).
    - Protokół/raport z audytu wewnętrznego (opracowany wspólnie z zespołem Zamawiającego).

Protokół/raport z przeglądu zarządzania (opracowany wspólnie z zespołem Zamawiającego).

Wykaz certyfikatów uprawniających do przeprowadzenia usługi:
1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
5) Certified Information Security Manager (CISM);
6) Certified in Risk and Information Systems Control (CRISC);
7) Certified in the Governance of Enterprise IT (CGEIT);
8) Certified Information Systems Security Professional (CISSP);
9) Systems Security Certified Practitioner (SSCP);
10) Certified Reliability Professional;
11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.