**Załącznik nr 1.1 do SWZ**

Pakiet nr 11 - Opracowanie oraz wdrożenie dokumentacji nowego Systemu Zarządzania Bezpieczeństwem Informacji.

Nazwa producenta: ……………

Typ, model, numer katalogowy: ………………

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **J.m.** | **Cena jednostkowa netto** | **Stawka podatku VAT** | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** | ***7*** | ***8*** |
| **1.** | Opracowanie oraz wdrożenie dokumentacji nowego Systemu Zarządzania Bezpieczeństwem Informacji | **Przedmiot zamówienia** |  |  |  |  |  |

|  |  |
| --- | --- |
| Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla SP ZOZ MSWiA w Szczecinie w oparciu o normę PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022, z uwzględnieniem analizy ryzyka na podstawie ISO/IEC 27005:2022 oraz dobrych praktyk z PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022), opracowanie rekomendacji, wytycznych oraz wsparciu i doradztwie dla Zamawiającego. | |
| Zakres usługi | * W ramach wdrożenia należy uwzględnić: * Analiza stanu bieżącego zarządzania bezpieczeństwem informacji Zamawiającego. * Wdrożenie wymagań w zakresie SZBI zgodnie z wytycznymi zawartymi w PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022); * Opracowanie i wdrożenie dokumentów według poniższej listy:   Wykaz zabezpieczeń technicznych i zabezpieczeń systemów informatycznych   * Polityka Bezpieczeństwa Informacji * Polityka czystego biurka i czystego ekranu * Polityka ciągłości działania w kontekście infrastruktury IT. * Analiza ryzyka w oparciu o ISO 27005 w zakresie infrastruktury IT. * Procedury wymagań w zakresie zabezpieczeń teleinformatycznych. * Procedura bezpiecznego przetwarzania informacji przez pracowników - Brak. * Procedura zabezpieczenia stacji roboczych. * Procedura nadawania, modyfikacji, odbierania uprawnień oraz przeglądu. * Procedura zarządzania dostępem do usług informatycznych. * Procedura zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami. * Procedura wymiany danych z podmiotami zewnętrznymi. * Procedura wewnętrznej wymiany danych. * Procedura postępowania z nośnikami informacji. * Procedura wprowadzania zmian w przetwarzaniu informacji. * Procedura zarządzania dokumentacją systemów informatycznych. * Procedura zgłaszania podatności. * Procedura postępowania z incydentami naruszenia bezpieczeństwa. * Procedura kontroli bezpieczeństwa informacji. * Procedura zarządzania oprogramowaniem. * Procedura zarządzania kopiami zapasowymi. * Procedura zarządzania kopiami archiwalnymi. * Procedura monitorowania bezpieczeństwa infrastruktury informatycznej. * Procedura przygotowania urządzeń IT do ponownego użycia. * Procedura wycofywania urządzeń IT z użycia. * Procedura bezpiecznego korzystania z urządzeń mobilnych. * Analizę ryzyka w oparciu o wytyczne zawarte w ISO/IEC 27005:2022, * Dobór i wdrożenie zabezpieczeń (kontroli) w oparciu o PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022), * Rekomendacje i wytyczne z zakresu dokumentacji, procedur i praktyk wynikające z normy PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022). * Wdrożenie procesów i procedur w środowisku Zamawiającego. * Szkolenie pracowników i kadry zarządzającej w zakresie nowych procedur oraz zasad wynikających z SZBI. * Przeprowadzenie audytu wewnętrznego, weryfikującego efektywność wdrożonego SZBI i wskazanie dalszych rekomendacji. * Doradztwo i wsparcie w zakresie utrzymania i ciągłego doskonalenia SZBI w okresie wdrożenia (bez formalnej certyfikacji). |
| Wdrożenie dokumentacji | Zamawiający nie dopuszcza kopiowania treści ogólnodostępnych w formie nieprzetworzonej (dostępnych w Internecie). Dokumenty będą zawierać przywołania zamiast cytowania tekstów analizowanych i powszechnie dostępnych. Dokumentacja ma zawierać wyłącznie autorskie treści, powstałe w wyniku realizacji zamówienia oraz inne autorskie treści wykonawcy, które nie są publicznie dostępne. Dokumenty będą opracowaniem kompletnym, wyczerpującym i dostosowanym do potrzeb organizacji, z punktu widzenia celu, któremu mają służyć. |
| Podstawa opracowania | * Norma PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022) – wymagania dla Systemu Zarządzania Bezpieczeństwem Informacji. * Norma PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022) – dobre praktyki i wytyczne w zakresie zabezpieczeń. * Norma ISO/IEC 27005:2022 – wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji. * Obowiązujące przepisy prawne w zakresie ochrony informacji i danych osobowych (np.KSC, KRI). * Dotychczas obowiązujące dokumenty wewnętrzne Zamawiającego (jeśli istnieją). |
| Cele wdrożenia | * Podniesienie poziomu bezpieczeństwa informacji poprzez wdrożenie sprawdzonych rozwiązań wynikających z ISO/IEC 27001 oraz ISO/IEC 27002. * Zarządzanie ryzykiem w sposób systematyczny, z wykorzystaniem ISO/IEC 27005 (od identyfikacji, przez analizę, aż do planowania sposobów postępowania z ryzykiem). * Zgodność z wymaganiami prawnymi w zakresie ochrony danych osobowych i bezpieczeństwa informacji. * Poprawa ciągłości działania kluczowych procesów biznesowych. * Stworzenie systemu zarządzania opartego na międzynarodowych standardach i najlepszych praktykach (ISO/IEC 27001, 27002, 27005). |
| Wymagania względem Wykonawcy | Kompetencje i doświadczenie zespołu   * Uprawnienia – co najmniej jedna osoba w zespole Wykonawcy posiadająca certyfikat audytora wiodącego ISO/IEC 27001. * Doświadczenie – minimum 2 zakończone wdrożenia SZBI w innych organizacjach. |
| **Metodyka realizacji** | * Praca w oparciu o wymagania norm PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022), PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022) oraz ISO/IEC 27005:2022. * Współpraca z zespołem roboczym po stronie Zamawiającego (przedstawiciele działu IT, kadr, prawnego itp.). * Regularne raportowanie postępów do Zamawiającego. * Prowadzenie dokumentacji projektowej (plan projektu, harmonogram, rejestr ryzyk, protokoły ze spotkań, raporty z wdrożeń). * Elastyczne dostosowanie ról: w zadaniach doradczych Wykonawca dostarcza wiedzę i wzorce; Zamawiający odpowiada za finalne przyjęcie i wdrożenie dokumentacji/procedur. |
| Etapy wdrożenia i harmonogram | Etap 1 – Analiza stanu obecnego Zadania:   * Przegląd istniejących polityk i procedur bezpieczeństwa informacji. * **Analiza dotychczasowych zabezpieczeń (technicznych, organizacyjnych, prawnych) w świetle PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022).** * **Wstępna identyfikacja luk (gap analysis) w odniesieniu do wymagań ISO/IEC 27001 i praktyk ISO/IEC 27002.** * Raport z analizy stanu bieżącego z zaleceniami do kolejnych etapów, rekomendacjami i planem dalszych działań.  Etap 2 – Planowanie SZBI i analiza ryzyka Zadania:   * Zdefiniowanie zakresu SZBI (obszary, procesy, zasoby). * Opracowanie/aktualizacja Polityki Bezpieczeństwa Informacji (PBI). * Analiza ryzyka (ISO/IEC 27005:2022): * Ustalenie kontekstu (kryteria ryzyka, poziomy akceptacji), * Identyfikacja i analiza zagrożeń i podatności, * Ocena skutków i prawdopodobieństwa, * Priorytetyzacja ryzyk, * Plan postępowania z ryzykiem (redukcja, akceptacja, przeniesienie, unikanie). * Wybór kontroli bezpieczeństwa z PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022) w kontekście zidentyfikowanych ryzyk i potrzeb Zamawiającego.   **Kamień milowy:**   * Zatwierdzona Polityka Bezpieczeństwa Informacji. * Raport z analizy ryzyka (wg ISO/IEC 27005) i wstępny plan postępowania z ryzykiem. * Wstępny dobór kontroli (środków zabezpieczeń) w oparciu o PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022).  Etap 3 – Opracowanie i wdrożenie dokumentacji Zadania:   * Przygotowanie dokumentacji SZBI na podstawie listy podanej w zakresie usługi oraz:   + Szczegółowych procedur bezpieczeństwa (np. zarządzanie dostępem, zarządzanie incydentami, ciągłość działania),   + Rejestru aktywów, rejestru ryzyk,   + Oświadczenie o Stosowalności (SoA) z uwzględnieniem PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022),   + Planu postępowania z ryzykiem,   + Instrukcji operacyjnych według potrzeb.   + Wdrożenia dokumentacji w środowisku Zamawiającego   + Szkolenia wstępne i instruktaże   + Ustalenie planu nadzoru i monitorowania (kontrole wewnętrzne, KPI, KRI, przeglądy kierownictwa).  Etap 4 – Testowanie, weryfikacja i doskonalenie Zadania:   * Testowanie procedur bezpieczeństwa (np. symulacja incydentów, awarii, testy odtwarzania systemów). * Weryfikacja skuteczności zabezpieczeń (dobranych wg ISO/IEC 27002) w kontekście założonych ryzyk i poziomów ochrony. * Monitorowanie wskaźników (KPI, KRI) i identyfikacja ewentualnych niezgodności. * Korekta i optymalizacja dokumentacji i procesów na podstawie wyników testów.   Kamień milowy:   * Raport z testów i weryfikacji procesów wraz z listą działań naprawczych lub usprawnień.  Etap 5 – Audyt wewnętrzny i finalizacja (styczeń 2026) Zadania:   * Audyt wewnętrzny SZBI (zgodnie z planem audytów). Wykonawca może przeprowadzić audyt lub wspierać zespół audytowy Zamawiającego. * Opracowanie raportu z audytu, wskazanie niezgodności i obszarów do doskonalenia. * Aktualizacja dokumentacji oraz procedur na podstawie wyników audytu (przy doradztwie Wykonawcy). * Szkolenia uzupełniające (jeśli zidentyfikowano nowe potrzeby).   Kamień milowy:   * Końcowy raport z audytu wewnętrznego. * Ostatecznie uzupełniona dokumentacja. * Plan ciągłego doskonalenia SZBI. |
| Produkty | W ramach realizacji zamówienia, Wykonawca (we współpracy z Zamawiającym) zobowiązuje się do dostarczenia lub współopracowania następujących produktów:   * Raport z analizy stanu obecnego (gap analysis). * Polityka Bezpieczeństwa Informacji oraz pakiet dokumentów SZBI (m.in. rejestry aktywów, rejestr ryzyk, procedury). * Kompletny proces analizy ryzyka (ISO/IEC 27005:2022): * Kryteria ryzyka i tolerancji, * Identyfikacja i analiza zagrożeń, * Ocena prawdopodobieństwa i skutków, * Plan postępowania z ryzykiem. * Dobór i opis kontroli ( PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022)) wraz z Oświadczeniem o Stosowalności (SoA). * Plan nadzoru i monitorowania SZBI (audyty wewnętrzne, przeglądy kierownictwa, KPI/KRI). * Raport z audytu wewnętrznego (jeżeli audyt przeprowadza Wykonawca) lub wsparcie w opracowaniu raportu (jeżeli audyt wykonuje zespół wewnętrzny Zamawiającego). * Zalecenia do dalszego doskonalenia SZBI po zakończeniu projektu. * Protokoły ze szkoleń i materiały szkoleniowe dla pracowników. |
| **Wymagania formalne i organizacyjne** | * Formy komunikacji – regularne spotkania (co 2–4 tygodnie), telekonferencje, wymiana dokumentów online. * Poufność – Wykonawca podpisuje NDA i zobowiązuje się do ochrony informacji Zamawiającego. * Rozdział zadań – w pracach o charakterze doradczym (np. tworzenie dokumentów, analiza ryzyka, dobór zabezpieczeń) Wykonawca zapewnia know-how i wzory; finalna implementacja, zatwierdzenie i formalna akceptacja jest po stronie Zamawiającego. |
| Kryteria odbioru prac | * Zgodność z normami PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022), PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022) i ISO/IEC 27005:2022 – wdrożony SZBI i proces analizy ryzyka muszą spełniać kluczowe wymagania tych norm. * Kompletność dokumentacji – dostarczenie wszystkich dokumentów wymienionych w punkcie 6. * Przeszkolenie personelu – potwierdzone przeprowadzenie szkoleń (listy). * Audyt wewnętrzny – potwierdzone przeprowadzenie i raport z wynikami audytu. * Zgodność z harmonogramem – zakończenie etapów w zaplanowanych terminach (dopuszczalne modyfikacje wynikające z uzgodnień między stronami). |
| Postanowienia końcowe | * Okres wsparcia po wdrożeniu 12 miesięcy. * Prawa własności – dokumentacja wytworzona w ramach projektu (z uwzględnieniem wzorów i szablonów) staje się własnością Zamawiającego; Wykonawca zachowuje prawa do wykorzystywanej metodyki czy opracowanych uniwersalnych wzorcach przed dostosowaniem do potrzeb Zamawiającego. * Brak obowiązku certyfikacji – usługa nie obejmuje formalnej certyfikacji, ale przygotowane rozwiązania umożliwią uzyskanie certyfikatu w przyszłości (po zakończeniu niezbędnych audytów zewnętrznych). |