WOJEWÓDZKI INSPEKTORAT INSPEKCJI HANDLOWEJ WE WROCŁAWIU
ul. Ofiar Oświęcimskich 15a, 50-069 Wrocław
tel. 71 3442038
e-doręczenia: AE:PL-72024-15247-AJRAE-30

SZCZEGÓŁOWY ZAKRES PRZEDMIOT ZAMÓWIENIA

Usługa kompleksowego opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w WIIH we Wrocławiu

przedmiotem zamówienia jest opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zapewniając doskonalenie podjętych działań i procedur w celu optymalizacji ryzyk związanych z naruszeniem poufności, dostępności, integralności oraz umożliwiającej pozytywne przejście procesu audytu zewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji na potrzeby WIIH we Wrocławiu.

Sporządzona dokumentacja w ramach realizacji zamówienia musi być zgodna z wymaganiami normy PN-EN ISO/IEC 27001:2023, Krajowych Ram Interoperacyjności (KRI) oraz Ustawy o Krajowym systemie cyberbezpieczeństwa „KSC" (tj. Dz.U. 2024, poz. 1077), w tym wdrożenie koniecznych rozwiązań wynikających z Dyrektywy NIS2.

Wymagany zakres:

ETAP I

Audyt wstępny - Analiza stanu istniejącego i określenie wymagań:

1. Realizacja audytu wstępnego mającego na celu m.in. szczegółową analizę obecnych procesów, procedur operacyjnych oraz mechanizmów kontroli związanych z bezpieczeństwem informacji, w celu zidentyfikowania istniejących luk organizacyjnych i procesowych oraz obszarów wymagających usprawnienia.
2. Przeprowadzenie audytu wstępnego z uwzględnieniem wszystkich komórek organizacyjnych audytowanej jednostki.
3. Przeprowadzenie wywiadu z pracownikami odpowiadającymi za bezpieczeństwo informacji, weryfikacja zgodności dokumentacji oraz procedur związanych z bezpieczeństwem informacji pod kątem wymagań aktualnej i obowiązującej normy PN-EN ISO/IEC 27001:2023, w tym Załącznika A do normy ISO/IEC 27001:2023 oraz wymagań Krajowych

Ram Interoperacyjności (KRI) oraz Ustawy o Krajowym systemie cyberbezpieczeństwa (KSC) i Dyrektywy NIS2, analiza luk, opracowanie raportu i koncepcji dalszych działań do zatwierdzenia przez Zamawiających.

4. Wykonawca wykona identyfikację ryzyk związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego
5. Wykonawca dokona oceny ryzyk i szans niezbędnych do zaprojektowania SZBI, również poprzez weryfikację działalności Zamawiającego m.in. w ich siedzibach (konieczność wizji lokalnej).
6. Wykonawca, po zakończeniu prac, sporządzi raport z przeprowadzonego Etapu I, zawierający propozycje rozwiązań i zmian w zakresie bezpiecznego przetwarzania informacji u Zamawiającego oraz obejmujący wstępne koncepcje SZBI, dostosowane do potrzeb Zamawiającego, w tym do ryzyk właściwych dla Zamawiającego zidentyfikowanych w wyniku przeprowadzonej Analizy, wskazując na główne obszary i rodzaje procedur, które powinny zostać uregulowane w SZBI. Raport powinien także uwzględniać opracowanie rejestru aktywów wykorzystywanych w danej instytucji wykorzystywanych do przetwarzania informacji.

ETAP II

Opracowanie, wdrożenie, przegląd i aktualizacja dokumentacji SZBI

Etap II będzie polegał na opracowaniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z wymaganiami normy ISO/IEC 27001:2023, obejmujące obszary funkcjonalne w Załączniku A do normy ISO/IEC 27001:2023, wymaganiami Krajowych Ram Interoperacyjności (KRI) oraz Ustawy o Krajowym systemie cyberbezpieczeństwa (KSC), w tym zaimplementowanie koniecznych rozwiązań wynikających z Dyrektywy NIS2 w WIIH we Wrocławiu. W ramach opracowania dokumentacji Wykonawca dokona pełnej analizy ryzyka wszystkich obszarów i systemów w oparciu o normę ISO/IEC 27001:2023 oraz zgodnie z najlepszymi praktykami i wytycznymi normy ISO/IEC 27005:2025. Po przeprowadzonej analizie ryzyka, zostanie przedstawione opracowanie zawierające kompletną ocenę ryzyka, w tym indywidualną ocenę ryzyka dla każdego aktywa zidentyfikowanego w Etapie I wraz z metodyką do dalszego wykorzystania przez Zamawiających (format .xlsx), która pozwoli na aktualizację zarządzania ryzykiem przez Zamawiających. Opracowanie będzie wykonane zgodnie ze specyfiką instytucji.

Etap II musi odzwierciedlać rzeczywistą strukturę organizacyjną, w tym procesów, procedur operacyjnych oraz mechanizmów kontroli związanych z bezpieczeństwem informacji oraz podział odpowiedzialności ich komórek organizacyjnych.

W etapie II finalnie Wykonawca przekaże w 2 egzemplarzach pełną, kompleksową dokumentację SZBI, zindywidualizowaną i dostosowaną do realizowanych przez nią procesów i zadań, zgodnej z wyżej wymienionymi regulacjami, w tym w szczególności z normą ISO/IEC 27001:2023 i Załącznikiem A do normy ISO/IEC 27001:2023. Zamawiający wymaga, aby dokumentacja została przygotowana w wersji papierowej i elektronicznej, w tym dodatkowo w wersji elektronicznej, edytowalna do aktualizowania i zarządzania wytworzonej dokumentacji przez Zamawiających.

ETAP III

Szkolenie

Przeprowadzenia szkoleń dotyczących wdrożonego SZBI, zapewniających kompleksowe zaznajomienie się z nowymi procedurami i politykami – ok 15 osób.

Szkolenie stacjonarne z możliwością dołączenia on-line. Wykonawca przekaże Zamawiającemu w ramach przedmiotu umowy materiały, w tym nagrane szkolenia dla pracowników do wielokrotnego wykorzystywania oraz wystawi certyfikaty lub zaświadczenia z odbytych szkoleń.

ETAP IV

Przygotowanie kompleksowego Planu Ciągłości Działania (PCD), który pozwoli na skuteczne reagowanie w sytuacjach kryzysowych oraz zapewni utrzymanie kluczowych procesów i usług w przypadku wystąpienia zdarzeń zakłócających.

W ramach Planu Ciągłości Działania Wykonawca zobowiązany będzie m.in. do:

1. przygotowania procedur awaryjnych i odtworzeniowych dla różnych scenariuszy kryzysowych (np. awarie systemów, brak dostępności obiektów, niedostępność kluczowych zasobów ludzkich),
2. określenia struktury organizacyjnej obowiązującej na czas kryzysu, w tym ról, odpowiedzialności, łańcucha decyzyjnego oraz kontaktów,
3. stworzenia planów komunikacji wewnętrznej i zewnętrznej, obejmujących pracowników, kontrahentów, media i interesariuszy,
4. przeprowadzenia co najmniej jednego testu scenariuszowego z Planu Ciągłości Działania oraz sporządzenia raportu z wynikami testu, zawierającego wnioski i rekomendacje dotyczące dalszego doskonalenia planu.