Załącznik nr 1 Opis potrzeb i wymagań Zamawiającego

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

Przedmiotem zamówienia jest „Usługa polegająca na przeglądzie, aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w Państwowej Inspekcji Pracy”.

Zamówienie dofinansowane ze środków Unii Europejskiej, Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności; Inwestycja: C3.1.1. Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; Cyberbezpieczeństwo - Cyberbezpieczny Rząd – w ramach projektu pn. „Cyberbezpieczeństwo w PIP", na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10- CR.01-001/24/0036/ KPOD.05.10-CR.01-001/25/2025"

1. Założenia dotyczące Zamówienia

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), w tym Polityki Bezpieczeństwa Informacji (dalej: PBI), zgodnego z:

1) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j.Dz.U.2024.1557 z późn.zm.) wraz z ustawą z dnia 25 lipca 2025 r. o

zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz.U.2025.1158);
2) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j.Dz.U.2024.1077) (dalej: KSC);
3) rozporządzeniem 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) (dalej: RODO);
4) rozporządzeniem 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 (Dz.U.2024.773) (dalej: KRI);
5) innymi niż ww. ustawami i rozporządzeniami, którym podlega Zamawiający w zakresie bezpieczeństwa informacji (z wyłączeniem ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2024.632 z pożn.zm.);
6) normą PN-EN ISO/IEC 27001:2023-08 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy Zarządzania bezpieczeństwem informacji. Wymagania” lub równoważną.

2. Zakres zamówienia

Podstawowe wymagania w zakresie zaprojektowania dokumentów, procedur i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), w tym Polityki Bezpieczeństwa Informacji (dalej: PBI) w Państwowej Inspekcji Pracy (dalej: PIP):

1) Realizacja Usługi zaprojektowania dokumentów, procedur i wdrożenia SZBI w tym PBI, obejmuje swoim zakresem:
    a) **Etap I –** Audyt SZBI (analiza luk zabezpieczeń, ocena podatności, ocena dokumentacji) – zidentyfikowanie stanu faktycznego, w tym stosowanych przez organizację technicznych i organizacyjnych zabezpieczeń, określenie obszarów do doskonalenia oraz harmonogramu dalszych prac;
    b) **Etap II** – Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji SZBI – określenie granic systemu zarządzania bezpieczeństwem informacji, celów, struktura organizacyjna systemu, kontekstu organizacji w tym analiza czynników zewnętrznych i wewnętrznych, stron zainteresowanych i ich wymagań, inwentaryzacja aktywów, wykonanie analizy ryzyka w zakresie bezpieczeństwa informacji, opracowanie/aktualizacja niezbędnej dokumentacji, w tym: polityki bezpieczeństwa informacji, mapy procesów, wymaganych procedur i formularzy, analiza odpowiednich zabezpieczeń i narzędzi służących bezpieczeństwu informacji;

c) **Etap III** – Audyt zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UoKSC), czyli weryfikacja stanu wdrożenia i funkcjonowania systemu zarządzania bezpieczeństwem informacji po wdrożeniu wymaganej dokumentacji w odniesieniu do przepisów prawa (KRI, UoKSC).

W celu zabezpieczenia przed nieuprawnionym dostępem osób trzecich, wszelkie informacje dotyczące realizacji usługi przekazywane będą poprzez uzgodniony pomiędzy Zamawiającym a Wykonawcą bezpieczny kanał komunikacji elektronicznej.

2) Zamawiający wymaga, aby Wykonawca do realizacji zamówienia skierował **co najmniej 2 osoby** w charakterze audytorów, z których każdy:
   a) posiada certyfikat - określony w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu - audytora wiodącego systemu zarządzania bezpieczeństwem informacji zgodnego z normą PN-EN ISO/IEC 27001 lub równoważny;
   b) posiada certyfikat - określony w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu - audytora wiodącego systemu zarządzania ciągłością działania zgodnego z normą PN-EN ISO 22301 lub równoważny;
   c) posiada minimum 2 letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa informacji;
   d) wykonał co najmniej 1 usługę audytu polegającą na przeprowadzaniu przeglądu, aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji.

3. Etap I – Audyt SZBI - Audyt przedwdrożeniowy

Zweryfikowanie poszczególnych komponentów funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji, w zakresie:

- ochrona danych osobowych;
- bezpieczeństwo zasobów ludzkich;
- bezpieczeństwo fizyczne i środowiskowe;
- bezpieczeństwo informacji;
- zapewnienie ciągłości działania PIP w sytuacjach kryzysowych, w zakresie bezpieczeństwa informacji.

poprzez:

- analizę aktualnej dokumentacji SZBI organizacji;
- analizę rozwiązań organizacyjnych wraz z realizowanymi obowiązkami;
- analizę stosowanych zabezpieczeń;
- raport z audytu stanowiący zestawienie obserwacji audytowych.

1) Wykonawca dokona audytu zgodności działań Zamawiającego z uregulowaniami prawnymi w zakresie bezpieczeństwa informacji wymienionych w pkt 1 ppkt 1-5 oraz z normą, o której mowa pkt 1 ppkt 6;
2) 7 dni przed rozpoczęciem prac Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy plan audytu przedwdrożeniowego. Plan audytu Wykonawca przekaże w formie elektronicznej na adresy email wskazane przez Zamawiającego;
3) Zakres prac audytu przedwdrożeniowego będzie obejmował co najmniej:
   a) zapoznanie się ze strukturą organizacyjną PIP;
   b) analizę i ocenę dokumentacji w zakresie bezpieczeństwa informacji, w tym polityk, procedur, zarządzeń, instrukcji oraz innych dokumentów, które Zamawiający udostępni Wykonawcy do analizy; Zamawiający zastrzega sobie prawo do udostępnienia dokumentacji wyłącznie w GIP lub poprzez wcześniej ustalony bezpieczny kanał komunikacji;
   c) wywiady analityczne z wyznaczonymi przez Zamawiającego i uzgodnionymi z Wykonawcą pracownikami komórek organizacyjnych GIP w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa określonych w KRI, normie PN-EN ISO/IEC 27001 lub równoważnej w tym uwzględniające:
      - kontekst organizacji,
      - organizację bezpieczeństwa informacji,
      - role, odpowiedzialność i uprawnienia,
      - działania odnoszące się do ryzyk i szans,
      - cele bezpieczeństwa informacji i plan ich osiągnięcia,
      - zarządzanie aktywami,
      - określenie praw dostępu do zasobów,
      - określenie kompetencji i poziomu uświadomienia pracowników,
      - postępowanie z ryzykiem w bezpieczeństwie informacji,
      - ocenę efektów działania poprzez monitoring, pomiary i analizę,
      - bezpieczeństwo zasobów ludzkich,
      - stosowanie metod zabezpieczeń (np. kryptografię),
      - bezpieczeństwo fizyczne i środowiskowe,
      - bezpieczną eksploatację,
      - bezpieczeństwo komunikacji,
      - pozyskiwanie i rozwój systemów,
      - zgodność oprogramowania z prawami autorskimi,
      - zarządzanie kopiami bezpieczeństwa;
      - zasady bezpieczeństwa sieci teleinformatycznej,
      - relacje z dostawcami (łańcuchy dostaw),
      - zarządzanie incydentami związanymi z bezpieczeństwem informacji,

- aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania,

d) obserwację budynków, pomieszczeń, działań i zachowań pracowników PIP, w celu weryfikacji przestrzegania przez nich obowiązującej polityki bezpieczeństwa informacji oraz wewnętrznych procedur z zakresu bezpieczeństwa informacji w PIP;

4) Wykonawca opracuje i sporządzi raport z przeprowadzonego audytu przedwdrożeniowego, zawierający w szczególności:
   a) cel i zakres audytu;
   b) szczegółowy opis przeprowadzonych prac;
   c) opis poziomu spełnienia każdego z wymagań bezpieczeństwa określonych w KRI, innych obowiązujących aktach prawnych o których mowa w pkt 1 ppkt 1-5, normie PN-EN ISO/IEC 27001 lub równoważnej oraz wewnętrznych uregulowaniach PIP;
   d) wykaz stwierdzonych niezgodności w odniesieniu do każdego wymagania określonego w KRI, innych obowiązujących aktach prawnych o których mowa pkt 1 ppkt 1-5, normie PN-EN ISO/IEC 27001 lub równorzędnej oraz wewnętrznych uregulowaniach Urzędu, na poziomie opisu poszczególnych zabezpieczeń wraz z przedstawieniem dowodów na istnienie niezgodności;
   e) rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do każdego z wymagań określonych w KRI, innych obowiązujących aktach prawnych o których mowa w pkt 1 ppkt 1-5, normie PN-EN ISO/IEC 27001 lub równoważnej oraz wewnętrznych uregulowaniach PIP;
   f) podsumowanie i wnioski.
5) Raport, o którym mowa w pkt 3 ppkt 4 Wykonawca przekaże Zamawiającemu w formie papierowej (podpisanej) w dwóch egzemplarzach oraz w formie elektronicznej podpisanej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym osoby upoważnionej do reprezentowania Wykonawcy. Raport w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem i przekaże go uzgodnionym z Wykonawcą bezpiecznym kanałem komunikacyjnym w terminie 30 dni od daty podpisania umowy.
6) Zamawiający zastrzega sobie prawo do wnoszenia uwag i wyjaśnień do przekazanego przez Wykonawcę raportu za pomocą uzgodnionego z Wykonawcą bezpiecznego kanału komunikacyjnego.
7) Ostateczną wersję raportu uwzględniającą uwagi i wyjaśnienia zgłoszone przez Zamawiającego, Wykonawca przekaże Zamawiającemu w terminie 30 dni od podpisania umowy.

4. Etap II - Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji SZBI.

1) Opracowanie niezbędnej dokumentacji/zapisów na podstawie zebranych informacji z Etapu I, w ścisłej współpracy z przedstawicielami Wykonawcy, obejmujący określenie:
   a) granic SZBI, interfejsów i powiązań,
   b) celów, czynników wewnętrznych i zewnętrznych,
   c) procesów zachodzących w PIP i ich wzajemnych zależności,
   d) ról, odpowiedzialności i uprawnień,
   e) niezbędnych kompetencji pracowników zajmujących się bezpieczeństwem informacji,
   f) inwentaryzację aktywów,
   g) analizy BIA (Business Impact Analysis – Analiza Wpływu Biznesowego), oceny ryzyka zakłóceń, planów ciągłości działania w zakresie bezpieczeństwa informacji,
   h) szacowania ryzyka w bezpieczeństwie informacji i ochronie danych osobowych,
   i) niezbędnej dokumentacji operacyjnej (polityki, procedury i instrukcje, ewidencje, rejestry, raporty itp. – niezbędnych do uzyskania pozytywnego efektu spełnienia wymagań określonych w przepisach w pkt. 1),
   j) adekwatnych zabezpieczeń i narzędzi służących bezpieczeństwu informacji i ochronie danych osobowych.
2) Zamawiający w ramach współpracy z Wykonawcą zobowiązuje się udostępnić poprzez bezpieczny kanał wymiany informacji posiadaną dokumentację PBI, jaka obowiązuje w Urzędzie, wraz z innymi dokumentami dotyczącymi bezpieczeństwa informacji.
3) Z uwagi na to, że PBI w PIP jest dokumentem służbowym dla użytku wewnętrznego, który zawiera informacje mogące mieć wpływ na bezpieczeństwo informacji oraz nie podlega udostępnianiu innym zewnętrznym podmiotom na zasadach określonych w odrębnych przepisach, wymagane będzie podpisanie dokumentu zachowania poufności przez Wykonawcę.
4) Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego w Etapie I, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest zaproponować organizację SZBI oraz opracować i przedstawić koncepcję wdrożenia zaktualizowanej PBI w PIP.
5) Koncepcja będzie w szczególności zawierać mapę dokumentów, stanowiącą szczegółowy wykaz dokumentów z zaznaczeniem ich wzajemnych powiązań, w tym: dokument PBI definiujący m.in. jej cele, podstawowe definicje, zakres atrybuty bezpieczeństwa informacji, wymogi prawne ochrony informacji, organizację i deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności pracowników PIP w zakresie bezpieczeństwa informacji, przeglądy polityk, m.in.:
   a) polityk bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w PIP w tym dla obszaru: teleinformatycznego, spraw

osobowych, zabezpieczeń fizycznych, ciągłości działania, ochrony danych osobowych, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;

b) regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

6) W przypadku dokumentów funkcjonujących w PIP, odnoszących się do bezpieczeństwa informacji, których zakres merytoryczny będzie w całości lub częściowo pokrywał się z opracowanymi przez Wykonawcę projektami dokumentów SZBI, Wykonawca zaproponuje i uzasadni sposób ich, wyłączenia, zastąpienia lub zintegrowania z zaproponowaną przez Wykonawcę mapą dokumentów.
7) Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uzasadnione uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia SZBI.
8) Na podstawie zatwierdzonej przez Zamawiającego koncepcji, o której mowa w pkt 4 ppkt 4)-5), Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty muszą być zgodne ze wszystkimi wymaganiami prawnymi, którymi podlega PIP. Jeżeli w czasie realizacji umowy zostaną uchwalone lub wydane akty prawne prawa powszechnie obowiązującego zmieniające wymagania prawa w zakresie bezpieczeństwa informacji, Wykonawca zobowiązany jest dostosować dokumentację SZBI do zaistniałych zmian. Na powyższy obowiązek nie wpływa fakt, że ww. akty prawne nie wejdą w życie podczas realizacji umowy.
9) Wszystkie dokumenty Wykonawca przekaże Zamawiającemu w formie papierowej (podpisanej) w dwóch egzemplarzach oraz w formie elektronicznej zostanie opatrzony kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym osoby upoważnionej do reprezentowania Wykonawcy. Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu w uzgodnionym z Zamawiającym bezpiecznym kanale komunikacji elektronicznej.
10) Zamawiający zastrzega sobie prawo do wnoszenia uzasadnionych uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.
11) Po należytym wykonaniu i realizacji etapu II zamówienia, który nie może trwać dłużej niż 30 dni kalendarzowych od momentu zakończenia etapu I, Zamawiający dokona rzeczywistej implementacji założeń wdrożeniowych w ramach swojej organizacji, przy aktywnym wsparciu Wykonawcy – a okres ten będzie wynosił maksymalnie 30 dni kalendarzowych od momentu zakończenia prac związanych z etapem II. Wsparcie

będzie obejmować m. in. spotkania robocze z pracownikami Zamawiającego, pokazanie dobrych praktyk, wskazanie działań newralgicznych, jak również zaprezentowanie zmian. Ewentualne spotkania będą odbywać się w formie online lub stacjonarnie – w siedzibie Zamawiającego w dniach roboczych – w terminach uzgodnionych i zaakceptowanych przez Wykonawcę i Zamawiającego.

5. Etap III. Wykonanie audytu SZBI pod względem zgodności zaktualizowanego systemu z KRI i UoKSC.

Audyt powdrożeniowy obejmuje następujące prace:

a) weryfikację poziomu wdrożenia w PIP zabezpieczeń zgodnie z rekomendacjami, o których mowa w pkt 3 ppkt 4 lit. e;
b) weryfikację stosowania zasad określonych w PBI przez pracowników Urzędu;
c) ocenę poziomu spełnienia wymagań KRI;
d) ocenę zgodności z przepisami zawartymi w aktach prawnych, wymienionych w pkt 1 ppkt 1-5 oraz z normą, o której mowa pkt 1 ppkt 6.

2) Audyt zostanie przeprowadzony w trzech wskazanych przez Zamawiającego jednostkach organizacyjnych PIP.
3) Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy plan audytu.
4) Wykonawca opracuje raport z audytu powdrożeniowego, zawierający co najmniej:
   a) cel i zakres przeprowadzonego audytu;
   b) opis przeprowadzonych prac;
   c) szczegółowy opis poziomu spełnienia wymagań KRI, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz normy PN-EN ISO/IEC 27001 lub równoważnej, w których podczas audytu przedwdrożeniowego stwierdzono niezgodności;
   d) potwierdzenie spełnienia wymogów określonych w przepisach zawartych w aktach prawnych wymienionych w pkt 1 ppkt 1-5 i normy o której mowa w pkt 1 ppkt 6, w tym potwierdzenie zgodności z przepisami RODO;
   e) wykaz zaobserwowanych niezgodności w odniesieniu do stosowania przez pracowników PIP zasad SZBI;
   f) szczegółowy opis działań korygujących i naprawczych;
   g) ogólną ocenę poziomu spełnienia wymagań KRI oraz normy PN-EN ISO/IEC 27001 lub równoważnej zgodnie z załącznikiem A do tej normy oraz poziomu stosowania przez pracowników Urzędu zasad SZBI;
   h) podsumowanie i wnioski.
5) Raport, o którym mowa w pkt 5 ppkt 4, Wykonawca przekaże Zamawiającemu w formie papierowej (podpisanej) w dwóch egzemplarzach oraz w formie elektronicznej podpisanej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub

podpisem osobistym osoby upoważnionej do reprezentowania Wykonawcy. Raport w formie elektronicznej Wykonawca zabezpieczy przed nieuprawnionym dostępem i przekaże go uzgodnionym z Wykonawcą bezpiecznym kanałem komunikacyjnym w terminie maksymalnie 60 dni od daty zakończenia Etapu II.

6) Zamawiający zastrzega sobie prawo do wnoszenia uwag i wyjaśnień do przekazanego przez Wykonawcę raportu za pomocą uzgodnionego z Wykonawcą bezpiecznego kanału komunikacyjnego. Wykonawca jest zobowiązany do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

6. Harmonogram realizacji zamówienia

1) Maksymalny termin realizacji – 120 dni od podpisania umowy**.**
2) Wykonawca zobowiązany jest zrealizować przedmiot zamówienie zgodnie z przedłożonym i zaakceptowanym harmonogramem rzeczowym.

7. Informacje o środowisku organizacyjnym i środowisku Państwowej Inspekcji Pracy

Środowisko organizacyjne:

Liczba osób pracujących około 2760 pracowników.

Struktura organizacyjna: PIP składa się z 18 głównych jednostek organizacyjnych: 16 okręgowych inspektoratów pracy, Ośrodka Szkolenia im. prof. Jana Rosnera we Wrocławiu oraz Głównego Inspektoratu Pracy, pełniącego rolę zarządczą. Dodatkowo większość okręgowych inspektoratów pracy posiada oddziały terenowe – łącznie 42 lokalizacje.

PIP nie posiada systemu zarządzania opartym na normach ISO. Obecnie wdrożony System Zarządzania Bezpieczeństwem Informacji jest wdrożony Polityką Bezpieczeństwa Informacji w PIP, który stanowi załącznik do Zarządzanie z dnia 19 grudnia 2018 r. Głównego Inspektora Pracy (dokument wewnętrzny nieudostępniany). PBI i SZBI było oparte na normie PN-EN ISO/IEC 27001:2017.