Ministerstwo Infrastruktury
Biuro Zarządzania Kryzysowego
ul. Chałubińskiego 4/6
00-928 Warszawa
tel.: 22 630 14 70

Opis Przedmiotu Zamówienia

I. ZAMAWIAJĄCY

Ministerstwo Infrastruktury
ul. Chałubińskiego 4/6
00-928 Warszawa

ePUAP: /MIIB/SkrytkaESP

Ministerstwo Infrastruktury jest urzędem administracji rządowej, obsługującym ministra właściwego działów administracji rządowej: transport, gospodarka morska, gospodarka wodna i żegluga śródlądowa. Stwarzamy warunki dla prawidłowego rozwoju tych działów i zapewniamy prawidłowe funkcjonowanie gospodarki i społeczeństwa. Kierujemy się dobrem wspólnym i wspieramy Ministra Infrastruktury w podejmowaniu decyzji, w oparciu o informacje przetwarzane w naszym Urzędzie. Ministerstwo mieści się w Warszawie w dwóch siedzibach: na ul. T. Chałubińskiego 4/6 oraz Nowy Świat 6/12. Informacje w Ministerstwie przetwarzane są w szczególności w systemach informatycznych Ministerstwa oraz w cyberprzestrzeni. Ministerstwo Infrastruktury zatrudnia ok 800 osób i realizuje zadania w ramach Departamentów, Biur, Państwowej Komisji Badania Wypadków Morskich i Państwowej Komisji Badania Wypadków Lotniczych,. Szczegółowe informacje dotyczące celów, zadań, struktury organizacyjnej oraz regulaminów znajdują się na stronie: https://www.gov.pl/web/infrastruktura/podstawowe-informacje

II. PRZEDMIOT ZAMÓWIENIA

Usługi konsultacyjne, doradcze, prace analityczne oraz audyt powdrożeniowy w zakresie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i usług IT w Ministerstwie Infrastruktury oraz jednostkach obsługiwanych tj.: Sekretariat Krajowej Rady Bezpieczeństwa Ruchu Drogowego, Państwowa Komisja Badania Wypadków Morskich, Państwowa Komisja Badania Wypadków Lotniczych

III. TERMIN REALIZACJI USŁUGI

Ustanowienie i wdrożenie SZBI oraz usług IT w Ministerstwie Infrastruktury potwierdzone protokołem końcowym odbioru przez Zamawiającego powinno zostać zrealizowane nie później niż w ciągu 335 dni kalendarzowych od podpisania umowy.

IV. SZCZEGÓŁOWY ZAKRES ZAMÓWIENIA

Wykonawca w ramach przedmiotu zamówienia będzie świadczyć usługi konsultacyjne, doradcze, prace analityczne oraz przeprowadzi audyt powdrożeniowy celem ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji wg ISO 27001 oraz usług IT w Ministerstwie Infrastruktury. Wykonawca kompleksowo przeprowadzi Zamawiającego przez proces wdrożenia systemowego podejścia do zarządzania bezpieczeństwem i ciągłością działania, poczynając od ustalenia kontekstu organizacji i celów bezpieczeństwa, po przygotowanie wymaganych normą ISO 27001 dokumentów a następnie ich wdrożenie. Zdefiniowanie usług IT oraz ich komponentów, określenie ich krytyczności oraz opracowanie planów ciągłości działania dla krytycznych usług IT.

Zamówienie uwzględnia charakter etapowy realizacji prac projektu „Ustanowienia i wdrożenia SZBI oraz usług IT" przy czym niektóre etapy mogą lub powinny być realizowane równolegle. Ogólny harmonogram prac wskazano w punkcie V OPZ. Szczegółowy harmonogram prac Wykonawca

przedstawi Zamawiającemu w ciągu 10 dni po podpisaniu umowy. Harmonogram szczegółowy może podlegać zmianom po zatwierdzeniu przez obie strony.

Etapy realizacji prac i warunki świadczenia usług:

1. Badanie stanu środowiska Zamawiającego pod kątem zgodności z obowiązującymi regulacjami prawnymi przed ustanowieniem i wdrożeniem SZBI oraz usług IT oraz przedstawienie oceny z badania w formie raportu.

2. Ustanowienie i wdrożenie „Polityki bezpieczeństwa informacji w Ministerstwie Infrastruktury", w tym analiza kontekstu wewnętrznego i zewnętrznego, ustalenie celów i mierników bezpieczeństwa.
   Opracowanie materiałów informacyjnych dot. wdrożenia nowej Polityki bezpieczeństwa informacji wprowadzającej SZBI, skierowanych do kierownictwa i pracowników Ministerstwa.

3. Wypracowanie metodyki zarządzania aktywami informacyjnymi w Ministerstwie, uwzględniającej cykl życia informacji, przypisanie właścicieli aktywów do realizowanych celów i zadań oraz działalności Ministerstwa.

   W pracach zaleca się korzystanie z normy ISO 27005. Wykonawca opracuje efektywny mechanizm pozwalający na przeprowadzenie identyfikacji i klasyfikacji aktywów. Prace dot. identyfikacji aktywów docelowo zostaną zawarte z rejestrze aktywów informacyjnych Ministerstwa. Wykonawca będzie wspierał Zamawiającego poprzez konsultacje w zakresie sposobu realizacji prac. Wykonawca przeprowadzi instruktaż dla kluczowych osób zaangażowanych w identyfikację aktywów w Ministerstwie w zakresie sposobu realizacji metodyki.

4. Opracowanie i wdrożenie metodyki zarządzania ryzykiem w oparciu o ISO 31000. Opracowanie metody autorskiej zarządzania ryzykiem, zdefiniowanie ról i zakresu odpowiedzialności. Przeprowadzenie procesu zarządzania ryzykiem i wdrożenie go w MI. Integracja procesu z innymi systemami (np. w zakresie ochrony danych osobowych, kontroli zarządczej), jeśli Zamawiający tak uzna po konsultacjach z Wykonawcą. Przeprowadzenie warsztatów z osobami zaangażowanymi bezpośrednio w proces zarządzania ryzykiem.

5. Wdrożenie dokumentacji SZBI wymaganej wg ISO 27001, tj. opracowanie i wdrożenie polityk dziedzinowych, procedur, instrukcji. Przeprowadzenie konsultacji dla całej organizacji. Wykonawca na podstawie wyników uzyskanych w trakcie realizacji badania, o którym mowa w pkt. 1, identyfikacji i klasyfikacji aktywów informacyjnych, identyfikacji usług IT oraz wyników szacowania ryzyka, przedstawi mapę dokumentów SZBI stanowiącą szczegółowy wykaz dokumentów z określeniem ich wzajemnych powiązań.

   Na podstawie zatwierdzonej przez Zamawiającego propozycji mapy dokumentów SZBI, Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty te muszą być zgodne ze wszystkimi wymaganiami prawnymi. Jeśli w trakcie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie Wykonawca zobowiązany jest dostosować dokumentację SZBI do zaistniałych zmian.

   Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

6. Identyfikacja i opisanie usług IT (w oparciu o ITIL) w Ministerstwie Infrastruktury. Wypracowanie podejścia do zarządzania usługami IT oraz opracowanie rejestru usług IT w Ministerstwie Infrastruktury.

7. Przeprowadzenie analizy wpływu na biznes określającej krytyczne aktywa MI, dopuszczalne czasy niedostępności usług IT, czas odtworzenia po katastrofie. Opracowanie i wdrożenie planów ciągłości dla usług IT lub ich komponentów.
   Zamawiający wymaga opracowania dokumentacji w liczbie zapewniającej pełne pokrycie zakresu realizowanych zadań IT w Ministerstwie.

8. Audyt powdrożeniowy. Wykonawca zapewni niezależnego audytora do przeprowadzenia audytu powdrożeniowego na zgodność ISO 27001, który dokona oceny funkcjonowania SZBI i przedstawi jego wyniki w raporcie z audytu.

V. OGÓLNY HARMONOGRAM REALIZACJI ZAMÓWIENIA

Etap I – Badanie przed ustanowieniem i wdrożeniem SZBI – do 14 dni od podpisania umowy.

Etap II – Wdrożenie Polityki bezpieczeństwa informacji w Ministerstwie – do 21 dni od podpisania umowy.

Etap III – Wdrożenie metodyki zarządzania aktywami informacyjnymi Ministerstwie – do 70 dni od zakończenia etapu II.

Etap IV – Wdrożenie metodyki zarządzania ryzykiem – do 70 dni od zakończenia etapu III.

Etap V – Wdrożenie pełnej dokumentacji SZBI zgodnej z ISO 27001 – prace powinny zostać rozpoczęte po realizacji etapu I, jednakże powinny być zrealizowane nie dłużej niż 75 dni od zakończenia etapu IV.

Etap VI – Identyfikacja i opisanie usług IT (w oparciu o ITIL) w Ministerstwie Infrastruktury. Wypracowanie podejścia do zarządzania usługami IT oraz opracowanie rejestru usług IT w Ministerstwie Infrastruktury. Prace powinny rozpocząć się po zrealizowaniu etapu IV, a realizacja ich powinna zakończyć się w ciągu 75 dni.

Etap VII – Opracowanie i wdrożenie planów ciągłości działania dla usług IT. Przeprowadzenie analizy wpływu na biznes – prace powinny rozpocząć się po zrealizowaniu etapu V i VI, a realizacja ich powinna zakończyć się w ciągu 75 dni.

Etap VIII – Audyt powdrożeniowy – prace powinny rozpocząć się po zrealizowaniu etapu VII, a realizacja ich powinna zakończyć się w ciągu 10 dni.

VI. WYMAGANE DOŚWIADCZENIE WYKONAWCY

1. Doświadczenie Wykonawcy w zakresie należytego wdrożenia SZBI w jednostkach administracji publicznej. Wykonawca w ostatnich 5 latach wykonał co najmniej jedną usługę wdrożenia lub aktualizacji SZBI obejmujące projekty wdrożenia zarządzania ryzykiem bezpieczeństwa informacji lub planowania ciągłości działania dla usług IT o wartości co najmniej 40 000 złotych polskich brutto każdy i potwierdzi to referencjami lub stosownymi dokumentami.
2. Wykonawca dysponuje dedykowanym zespołem ekspertów do realizacji zakresu prac tj.: co najmniej dwóch ekspertów posiadających niezbędną wiedzę i doświadczenie w zakresie realizacji projektu. Każdy ekspert powinien posiadać przynajmniej jeden certyfikat wskazany w wykazie certyfikatów uprawniających do przeprowadzenia audytu (Załącznik do rozporządzenia Ministra Cyfryzacji z dnia 12.10.2018 do ustawy o ksc). Co najmniej jeden ze wskazanych ekspertów powinien posiadać doświadczenie z zakresu wdrożenia biblioteki dobrych praktyk IT – ITIL lub stosowania metodyki COBIT, potwierdzone stosownymi referencjami. Prosimy o dołączenie opisu doświadczenia zawodowego ekspertów, którzy są dedykowani do realizacji niniejszego zamówienia.
3. Wykonawca wskaże kierownika projektu, jako osoby wiodącej spośród wskazanych ekspertów. Osoba pełniąca funkcję kierownika projektu powinna posiadać 4 letnie doświadczenie zawodowe, rozumiane jako udział w projektach informatycznych i co najmniej

2 letnie doświadczenie zawodowe w zakresie funkcji kierownika lub zastępcy kierownika projektu w ciągu ostatnich 8 lat.

VII. ORGANIZACJA REALIZACJI OPISU PRZEDMIOTU ZAMÓWIENIA

1. Kierownik projektu będzie posiadał pełną wiedzę o realizowanym projekcie oraz będzie odpowiedzialny za komunikację w projekcie i podpisywanie raportów cząstkowych z etapów realizacji prac, przedstawianie harmonogramów oraz ewentualnych zmian.
2. W ramach każdego etapu Wykonawca przeprowadzi przynajmniej jedno spotkanie inicjujące, na którym poinformuje w szczególności o harmonogramie pracy, sposobie realizacji, celach, produktach cząstkowych, kamieniach milowych.
3. W ramach etapów II-VII Wykonawca powinien przewidzieć konsultacje w siedzibie Zamawiającego w liczbie nie mniejszej niż 50 godzin. W sytuacji wprowadzenia pracy zdalnej u Zamawiającego lub z innych ważnych przyczyn, Zamawiający dopuszcza by konsultacje i spotkania inicjujące kolejne etapy projektu realizowane były on-line za pomocą MS-Teams.
4. Wykonawca wymaga informowania w formie pisemnej o przebiegu realizacji prac z uwzględnieniem każdego etapu, o którym mowa w punkcie V OPZ.
5. Każdy etap prac uznaje się za zakończony po przyjęciu przez obie strony raportu z zakończenia prac danego etapu.
6. Informacje, które będą przekazywane w celu realizacji niniejszego projektu, stanowią informacje chronione, w związku z tym realizacja projektu będzie wymagała akceptacji zapisów o zachowaniu poufności i zapewnieniu stosownej ochrony, w tym również dla danych osobowych.
7. Wszystkie dokumenty sporządzone będą w formie pisemnej w języku polskim, w formie papierowej oraz formie elektronicznej w formacie danych .pdf oraz jednym z formatów edytowalnych: .doc, .rtf, .xlsx.
8. Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty niniejszego zamówienia.
9. Wykonawca w ramach 12 miesięcznej gwarancji, liczonej od dnia zakończenia ostatniego etapu, zobowiązany będzie do poprawy błędów w przekazanej dokumentacji niezależnie od jej formy wytworzenia, w terminie nie dłuższym niż 30 dni od daty zgłoszenia błędu przez Zamawiającego.

VIII. KARY

Zamawiający przewiduje w umowie kary, w następujących przypadkach:

1. W przypadku przekroczenia terminu realizacji, o którym mowa w rozdziale III, Zamawiający przewiduje karę finansową w wysokości 100 zł za każdy rozpoczęty dzień zwłoki.
2. Zwłoki w usunięciu wad stwierdzonych przy odbiorze, w stosunku do 30-dniowego terminu na ich sprostowanie, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 100 złotych za każdy rozpoczęty dzień.
3. Naruszenia bezpieczeństwa informacji (w tym przepisów dotyczących ochrony danych osobowych) ze strony Wykonawcy, Zamawiający przewiduje karę finansową w wysokości 20 000 złotych za każdy przypadek.

IX. DOKUMENTY WYTWORZONE W RAMACH REALIZACJI PROJEKTU

Dokumenty operacyjne:

1. Raport z badania przed ustanowieniem i wdrożeniem SZBI.
2. Polityka bezpieczeństwa informacji.
3. Materiały informacyjne dot. PBI.
4. Ankieta skierowana do właścicieli aktywów.
5. Metodyka identyfikacji aktywów wraz z dokumentami operacyjnymi.
6. Rejestr aktywów zgodnie z ISO 27005.
7. Metodyka zarządzania ryzykiem wraz z dokumentami operacyjnymi.
8. Rejestr ryzyk IT.

9. Mapa dokumentów SZBI.
10. Pełna dokumentacja SZBI (około 8 dokumentów).
11. Rejestr usług IT.
12. Ankieta BIA.
13. Plany ciągłości działania dla usług IT (około 6 dokumentów).
14. Raport z audytu powdrożeniowego.

Dokumenty zarządcze:

1. Harmonogram realizacji etapów I-VII.
2. Notatki ze spotkań.
3. Raporty z realizacji prac etapów.
4. Raport końcowy.