Załącznik nr 1

Opis Przedmiotu Zamówienia (OPZ).

Projekt grantowy pn. ***„CYBERBEZPIECZNY SAMORZĄD”*** o numerze FERC.02.02-CS.01-001/23 realizowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) w ramach Priorytetu II: Zaawansowane usługi cyfrowe, Działania 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa .
Umowa o powierzenie grantu o numerze **FERC.02.02-CS.01-001/23/0939/ FERC.02.02-CS.01-001/23/2024** z dnia 12.04.2024 r.
OPZ dotyczy „Opracowania, wdrożenia, przeglądu, aktualizacji i utrzymania dokumentacji SZBI dla Urzędu Miejskiego w Lubinie” oraz „Opracowania, wdrożenia, przeglądu, aktualizacji i utrzymania dokumentacji SZBI dla Miejskiego Ośrodka Pomocy Społecznej w Lubinie”. Zadanie 1 – Obszar organizacyjny.

Kod CPV: 79417000-0 Usługi doradcze w zakresie bezpieczeństwa

Część 1

„Opracowanie, wdrożenie, przegląd, aktualizacja i utrzymanie dokumentacji SZBI dla Urzędu Miejskiego w Lubinie”.

Urząd Miejski w Lubinie mieści się w trzech budynkach:

1. Ratusz - ul. Rynek 25, 59-300 Lubin – 6 pracowników;
2. Budynek Główny – ul. Kilińskiego 10, 59-300 Lubin – 135 pracowników;
3. Referat Lokalowy – ul. Rzeźnicza 1, 59-300 Lubin – 9 pracowników.

Na stronach BIP pod adresem:
https://bip.um.lubin.pl/artykuly/regulamin-organizacyjny
znajduje się aktualny Regulamin Organizacyjny Urzędu oraz struktura organizacyjna Urzędu z podziałem na etaty.

Przedmiotem zamówienia jest wdrożenie w Urzędzie Miejskim w Lubinie, Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301.
Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:

- rozporządzenia 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 ;
- ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa;
- rozporządzenia 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).

Wykonawca zobowiązany jest do wytworzenia dokumentacji, formularzy, opracowania zasad postepowania, procedur itd., które będą zgodne z zapisami Regulaminu Konkursu Grantowego oraz Wzorem Umowy o powierzeniu Grantu dostępnych na stronie:

https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

Część 2

„Aktualizacja i wdrożenie dokumentacji SZBI dla Miejskiego Ośrodka Pomocy Społecznej w Lubinie (MOPS)".

Miejski Ośrodek Pomocy Społecznej w Lubinie z siedzibą przy ul. Kilińskiego 25A zatrudnia łącznie 177 pracowników, a w jego strukturze organizacyjnej znajdują się 3 jednostki organizacyjne:

- Żłobek Nr 2, ul. Cedyńska 13, 59-300 Lubin (30 pracowników);
- Żłobek Nr 3, ul. Orla 47, 59-300 Lubin (19 pracowników);
- DDP "Senior", ul. Henryka Sienkiewicz 3, 59-300 Lubin (10 pracowników).

Przedmiotem zamówienia jest analiza, aktualizacja i wdrożenie wprowadzonej w MOPS w Lubinie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w sposób gwarantujący spełnienie wymagań norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301.
Na bazie wprowadzonej w MOPS Lubin Polityki Bezpieczeństwa Informacji Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:

- rozporządzenia 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 ;
- ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa;
- rozporządzenia 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).

Wykonawca zobowiązany jest do wytworzenia dokumentacji, formularzy, opracowania zasad postępowania, procedur itd., zgodnie z wymaganiami opisanymi w dalszej części niniejszego dokumentu. Wdrożony przez Wykonawcę SZBI musi gwarantować spełnienie wymagań stawianych Zamawiającemu zapisami Regulaminu Konkursu Grantowego oraz Wzorem Umowy o powierzeniu Grantu dostępnych na stronie:
https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

Część 3.

Wymagania dotyczące realizacji zadań określonych w Części 1 oraz w Części 2

I. Ogólny zakres zadań Wykonawcy:

1. Wykonanie audytu wstępnego obejmującego min.:
   - inwentaryzację uprawnień w programach i systemach informatycznych,
   - inwentaryzację aktywów,
   - rozpoznanie struktury organizacyjnej i realizowanych procesów oraz wymagań prawnych funkcjonowania jednostki.

2. Stworzenie dokumentacji SZBI z uwzględnieniem istniejących procedur.
3. Opracowanie zasad i formularzy dotyczących nadawania i odbierania uprawnień w programach informatycznych.
4. Aktywny udział w inwentaryzacji aktywów oraz przypisaniu własności aktywów.
5. Analiza ryzyka i opracowanie planu postępowania z ryzykiem.
6. Dostosowanie procedur do istniejącego ryzyka.
7. Opracowanie planu ciągłości działania.
8. Przeprowadzenie, w siedzibie Zamawiającego, szkolenia dla wszystkich pracowników Zamawiającego oraz Miejskiego Ośrodka Pomocy Społecznej w Lubinie z zakresu funkcjonowania i stosowania SZBI. Szkolenia odbywać się będą w grupach do 30 osób.
9. Opracowanie działań korygujących i zapobiegawczych.
10. Przygotowanie harmonogramu przeglądów funkcjonowania SZBI.

II. Sposób realizacji zadania:

1. Zamawiający wymaga aby wszystkie prace związane z przeprowadzaniem wywiadów, ankiet i analiz wśród pracowników Zamawiającego realizowane były przez przedstawiciela Wykonawcy w siedzibie Zamawiającego; Zamawiający wyklucza możliwość stosowania ankiet do samodzielnego wypełnienia przez pracowników Zamawiającego.
2. Wykonawca zobowiązany jest do stawiennictwa w siedzibie Zamawiającego na każde jego żądanie związane z realizacją przedmiotu zamówienia.

Podstawą do oceny Polityki Bezpieczeństwa Informacji będzie dodatkowe zestawienie dostarczone przez Wykonawcę, bazujące na załączniku A do normy ISO/IEC 27001 pokazujące wszystkie pozycje powołanego załącznika wraz z informacją który obszar wdrożonej dokumentacji reguluje poszczególne jego zagadnienia. Szablon tego zestawienia zostanie określony przez Zamawiającego.

III. Wymagania stawiane wykonawcy:

1. Potwierdzenie, że w ciągu ostatnich trzech lat wykonał wdrożenie SZBI (lub dokonał jej dostosowania do aktualnych wymogów prawnych) w 2 jednostkach budżetowych (urzędy miast i gmin, starostwa oraz ośrodki pomocy społecznej).
2. Wykonawca musi dysponować i przeznaczyć do realizacji zamówienia co najmniej jedną osobę będącą audytorem posiadającym przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999).

Dla potwierdzenia powyższego Wykonawca przedłoży wraz z ofertą załącznik nr 4 wykaz osób wraz z dokumentami potwierdzającymi spełnianie warunku. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają łącznie warunki w zakresie wykonania usług oraz wyznaczenia osób do realizacji zamówienia

IV. Wymagania dotyczące Polityki Bezpieczeństwa Informacji:

Zamawiający wymaga aby wdrożona Polityka Bezpieczeństwa Informacji w sposób usystematyzowany oraz jednoznaczny opisywała i regulowała wymienione niżej zagadnienia oraz obszary funkcjonowania wynikające bezpośrednio z celów stosowania zabezpieczeń stanowiących załącznik A do normy ISO/IEC 27001.

Polityka Bezpieczeństwa Informacji (zagadnienia ogólne):

- znaczenie bezpieczeństwa informacji dla organizacji
- cele jakie organizacja zamierza osiągnąć w zakresie bezpieczeństwa informacji,
- obszar stosowania polityki,
- zgodność z obowiązującymi przepisami i normami.

Organizacja bezpieczeństwa informacji:

- role i odpowiedzialność za bezpieczeństwo informacji,
- rozdzielanie obowiązków,
- bezpieczeństwo informacji w zarządzaniu projektami,
- polityka stosowania urządzeń mobilnych,
- telepraca.

Bezpieczeństwo zasobów ludzkich:

- postępowanie sprawdzające przed zatrudnieniem,
- warunki zatrudnienia,
- odpowiedzialność kierownictwa,
- uświadamianie i szkolenia z zakresu bezpieczeństwa informacji
- zakończenie zatrudnienia i zmiana zakresu obowiązków.

Zarządzanie aktywami:

- inwentaryzacja aktywów,
- własność aktywów,
- akceptowalne użycie aktywów,
- zwrot aktywów,
- klasyfikowanie informacji
- oznaczanie informacji
- postępowanie z aktywami,
- zarządzanie nośnikami wymiennymi,
- wycofywanie nośników,
- przekazywanie nośników.

Kontrola dostępu:

- polityka kontroli dostępu,
- dostęp do sieci i usług sieciowych,
- rejestrowanie i wyrejestrowanie użytkowników,
- przydzielanie dostępu użytkownikom,
- zarządzanie prawami uprzywilejowanego dostępu (w tym zasady funkcjonowania administratorów podstawowych, takich jak np.: admin, administrator, root),
- przegląd praw dostępu użytkowników,
- odbieranie lub dostosowanie praw dostępu,
- stosowanie poufnych informacji uwierzytelniających,
- ograniczanie dostępu do informacji.

- procedury bezpiecznego logowania,
- system zarządzania hasłami,
- użycie uprzywilejowanych programów narzędziowych,
- kontrola dostępu do kodów źródłowych programów,

Kryptografia:

- polityka stosowania zabezpieczeń kryptograficznych,
- zarządzanie kluczami.

Bezpieczeństwo fizyczne i środowiskowe.

- fizyczna granica obszaru bezpiecznego,
- fizyczne zabezpieczenie wejść,
- zabezpieczenie biur, pomieszczeń i obiektów,
- ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
- praca w obszarach bezpiecznych,
- obszary dostaw i załadunku,
- lokalizacja i ochrona sprzętu,
- systemy wspomagające,
- bezpieczeństwo okablowania,
- konserwacja sprzętu,
- wynoszenie aktywów,
- bezpieczeństwo sprzętu i aktywów poza siedzibą,
- bezpieczne zbywanie lub przekazywanie do ponownego użycia
- pozostawienie sprzętu użytkownika bez opieki,
- polityka czystego biurka i czystego ekranu.

Bezpieczna eksploatacja:

- dokumentowanie procedur eksploatacyjnych,
- zarządzanie zmianami,
- zarządzanie pojemnością,
- zabezpieczenia przed szkodliwym oprogramowaniem,
- kopie zapasowe,
- rejestrowanie zdarzeń,
- ochrona informacji w dziennikach zdarzeń,
- rejestrowanie działań administratorów i operatorów,
- synchronizacja zegarów,
- instalacja oprogramowania w systemach produkcyjnych,
- zarządzanie podatnościami technicznymi,
- ograniczenia w instalowaniu oprogramowania

Bezpieczeństwo komunikacji:

- zabezpieczenia sieci,
- bezpieczeństwo usług sieciowych,
- rozdzielanie sieci,

- polityki i procedury przesyłania informacji,
- wiadomości elektroniczne

Pozyskiwanie, rozwój i utrzymanie systemów:

- analiza i specyfikacja wymagań bezpieczeństwa informacji,
- zabezpieczanie usług aplikacyjnych w sieciach publicznych,
- procedury kontroli zmian w systemach.

Analiza ryzyka:

- strategia zarządzania ryzykiem - opis konkretnych działań odnoszących się do zarządzania ryzykiem, w tym: opis procesu, narzędzia i techniki, role i zakresy odpowiedzialności, skala oceny prawdopodobieństwa i wpływu ryzyka, progi tolerancji na ryzyko, kategorie ryzyka, szablony (wzory dokumentów) niezbędne w zarządzaniu ryzykiem, kluczowe wskaźniki efektywności i wskaźniki wczesnego ostrzegania, harmonogram działań, raportowanie,
- diagnoza ryzyka - identyfikacja ryzyk pozwalająca ocenić sytuację i zdarzenia pod kątem ich możliwego wpływu na bezpieczeństwo informacji,
- analiza i ocena - analiza ryzyka (ocena) z wykorzystaniem metody oceny jakościowej/ilościowej,
- monitorowanie ryzyka,
- rejestr ryzyk.

Plan ciągłości działania:

- identyfikacja kluczowych zasobów, procesów, usług i dostawców,
- scenariusze utraty ciągłości działania,
- zasady komunikacji w sytuacjach kryzysowych,
- plany przywracania ciągłości działania,
- redundancja zasobów i usług kluczowych,
- zasady testowania planu.

V. Ochrona danych osobowych:

Zamawiający wymaga aby zagadnienia związane z ochroną danych osobowych opracowane były w wydzielonym dokumencie (nowa *Polityka Ochrony Danych Osobowych przetwarzanych w Urzędzie Miejskim w Lubinie*). Zamawiający wymaga aby dokument ten zawierał w szczególności:

- struktura organizacji ochrony danych osobowych,
- zasady przekazywania danych odbiorcom (zasady powierzenia i udostępnienia danych),
- zasady privacy by design oraz privacy by defalut,
- zasady retencji danych osobowych,
- procedura szkoleń oraz nadawania upoważnień do przetwarzania danych,
- procedura postępowania z incydentami związanymi z ochroną danych osobowych,
- procedura oceny skutków dla ochrony danych osobowych (DPIA),
- procedura realizacji praw osób, których dane dotyczą,
- procedura audytu zgodności przetwarzania danych osobowych,
- opis organizacyjnych środków bezpieczeństwa,
- opis fizycznych środków bezpieczeństwa,

- opis technicznych środków bezpieczeństwa,
- wzory ewentualnych formularzy do powyższych zasad i procedur.

VI. Wymagania dotyczące polityki bezpieczeństwa systemu informatycznego:

Zamawiający wymaga aby wszystkie zagadnienia odnoszące się bezpośrednio do systemu informatycznego opracowane były w wydzielonym dokumencie do zapisów którego odnosić się będą zarówno Polityka Bezpieczeństwa Informacji oraz dokument opisujący zasady ochrony danych osobowych. Zamawiający wymaga aby dokument ten regulował następujący (minimalny) zakres działań/zagadnień:

- nadawanie uprawnień użytkownikom systemów informatycznych należących do Zamawiającego w sposób precyzyjny i jednoznaczny, umożliwiający wykonywanie okresowej kontroli uprawnień w programach i systemach informatycznych,
- zasady nadawania uprawnień uprzywilejowanych (ASI),
- nadawanie uprawnień w systemach informatycznych niepodlegających nadzorowi ze strony administratora lokalnego (np. ZUS PUE, GUS, ePUAP),
- organizacja certyfikatów SSL,
- organizacja kluczy szyfrujących,
- zasady użytkowania zewnętrznych nośników informacji,
- zasady użytkowania komputerów mobilnych,
- zasady wykonywania pracy zdalnej przez pracowników Zamawiającego,
- zasady nawiązywania połączeń zdalnych przez wsparcie techniczne producentów programów (w trybie nadzorowanym i nienadzorowanym),
- zasady nawiązywania połączeń zdalnych przez Administratorów Systemu Informatycznego,
- archiwizacja danych i testowanie kopii bezpieczeństwa,
- kontrola dostępu do sieci, systemu i aplikacji,
- użytkowanie i zabezpieczenia stanowiska użytkownika,
- bezpieczeństwo fizyczne i środowiskowe,
- kontrola połączeń z siecią publiczną,
- zasady wykorzystania zabezpieczeń kryptograficznych,
- aktualizacja i testowanie oprogramowania.

Dokumentacja opisująca zasady funkcjonowania i kontroli systemu informatycznego powinna zawierać szablony wszystkich wykazów i rejestrów które powinny być prowadzone przez użytkowników lub administratorów systemu informatycznego.

VII. Harmonogram i rozliczenie prac.

Rozliczenie prac nastąpi w trzech etapach po wykonaniu prac opisanych w Części 3 punkcie I Ogólnym zakresie zadań Wykonawcy:

1. Punkty 1-3 – płatność 40% oferowanej ceny. Termin wykonania tej części zadania nie może przekroczyć trzech miesięcy od zawarcia umowy.
2. Punkty 4-7 - płatność 30% oferowanej ceny. Termin wykonania tej części zadania nie może przekroczyć sześciu miesięcy od zawarcia umowy.
3. Punkty 8-10 - płatność 30% oferowanej ceny.

Termin wykonania całości zadania nie może przekroczyć 31 grudnia 2025 roku.

Wykonawca określi terminy wykonania poszczególnych etapów.