Ogłoszenie

Numer

2024-20934-193315

Id

193315

Powstaje w kontekście projektu

FERC.02.02-IP.01-0001/23 - Cyberbezpieczna Gmina Mirsk

Tytuł

Cyberbezpieczna Gmina Mirsk Zadanie 1 i Zadanie 2

Załączniki

Dodane do ogłoszenia w obowiązującej wersji z dn. 2024-07-09
1. Pełna treść ogłoszenia
2. Załącznik nr 1 -PDF
3. Załącznik nr 1 w formie edytowalnej
4. Załącznik nr 2

Czy dopuszczalna oferta częściowa?

NIE

Data opublikowania ogłoszenia

2024-07-09

Data ostatniej zmiany

2024-07-09

Termin składania ofert

2024-07-12 11:00:00

Planowany termin podpisania umowy

2024-07

Dane adresowe ogłoszeniodawcy

> Gmina Mirsk
> Plac Wolności Plac Wolności
> 59-630 Mirsk
> NIP: 6161008487

Osoby do kontaktu

Alicja Jaszczyszyn
tel.: 75 62 22 169
e-mail: rodo@mirsk.pl

Części zamówienia

Część: 1

Tytuł części 1

Cyberbezpieczna Gmina Mirsk Zadanie 1 i Zadanie 2

Czy dopuszczalne oferty wariantowe

NIE

Przedmioty zamówienia do części 1

Typ

Usługa

Podkategoria

Usługi inne

Opis

Zamówienie obejmuje dwa obszary działania w ramach realizacji zadania Cyberbezpieczna Gmina Mirsk. Przedmiot zamówienia będzie realizowany dla Urzędu Miasta i Gminy Mirsk, Zakładu Gospodarki Komunalnej i Mieszkaniowej w Mirsku, a także Miejsko Gminnego Ośrodka Pomocy Społecznej w Mirsku.
4. Przewidywany podział na części:
Część 1 – Zadanie 1 Obszar organizacyjny: Przedmiotem zamówienia dla Części 1 jest usługa wykonania wstępnego audytu bezpieczeństwa informacji dla Zamawiającego oraz wsparcie w wypełnieniu „Ankiety dojrzałości Cyberbezpieczeństwa”, która stanowi załącznik nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”. Następnie Wykonawca zrealizuje wdrożenie w Urzędzie Miasta Gminy Mirsk, a także podległych jednostkach organizacyjnych systemu zarządzania

bezpieczeństwem informacji (SZBI). Dokumentacja SZBI musi obejmować bezpieczeństwo fizyczne (ochrona pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), bezpieczeństwo technologiczne (bezpieczeństwo systemu teleinformatycznego) oraz bezpieczeństwo osobowe i organizacyjne. Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023;
- Norma PN-EN ISO/IEC 22301:2020.

W ramach zadania Wykonawca opracuje oddzielny system dla każdej jednostki, który będzie obejmował m.in. wdrożenie dokumentacji, w tym niezbędnych polityk, procedur i instrukcji, przeprowadzenie szkolenia zespołu wdrożeniowego Zamawiającego w zakresie systemu zarządzania bezpieczeństwem informacji oraz zapewnienie wsparcia dla zespołu wdrożeniowego SZBI Zamawiającego.

Dodatkowo Wykonawca wykona okresowy audyt KRI (po wdrożeniu SZBI) zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Ustawą o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018r. (Dz. U. 2023 r. poz. 913), Normą ISO/IEC 27001, Normą PN-EN ISO/IEC 22301

Audyt ma obejmować weryfikację bezpieczeństwa:

- fizycznego (sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp)
- bezpieczeństwa informatycznego (analiza bezpieczeństwa systemu teleinformatycznego)
- bezpieczeństwa organizacyjnego (stosowanie procedur bezpieczeństwa), w tym przegląd dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji.

W ramach przeprowadzonych audytów Wykonawca przeprowadzi weryfikację:

- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji,
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem,

uszkodzeniami lub zakłóceniami,
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
- zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
- zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
- bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Wykonawca dostarczy Zamawiającemu:
- wstępnie wypełnioną „Ankietę Dojrzałości Cyberbezpieczeństwa" oraz z finalnie uzupełnioną o stan i opis zrealizowanych zmian po zakończeniu zadania.
- raporty z audytów bezpieczeństwa informacji (dotyczy audytu wstępnego oraz okresowego) wraz z rekomendacjami do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.
- opracowany, opublikowany, zakomunikowany pracownikom i właściwym stroną zewnętrznym oraz aktualizowany na bieżąco zgodnie z zewnętrznymi wymaganiami System Zarządzania Bezpieczeństwem Informacji (SZBI).

Część 2 – Zadanie 2 Obszar kompetencyjny: Szkolenie pracowników i audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji z zakresu cyberbezpieczeństwa. Opracowanie kompleksowego programu szkoleniowego z zakresu cyberbezpieczeństwa w celu zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa wszystkich pracowników. Szkolenie audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji. Przeprowadzenie testów socjotechnicznych poprzez rozesłanie na adresy e-mail służbowe pracowników wiadomości pozorujących przeprowadzenie ataku socjotechnicznego. Audytor będzie mógł sprawdzić ilu pracowników otworzy linki sprawdzające oraz od ilu pracowników byłby w stanie uzyskać hasła dostępowe.
Szkolenia muszą być zrealizowane w siedzibie:
- Urzędu Miasta i Gminy Mirsk - Plac Wolności 39, 59-630 Mirsk
- Zakładu Gospodarki Komunalnej i Mieszkaniowej w Mirsku – ul. A. Mickiewicza 38, 59-630 Mirsk
- Miejsko Gminnego Ośrodka Pomocy Społecznej w Mirsku – Plac Wolności 40, 59-630 Mirsk

Co najmniej 4 tury szkolenia dla każdej jednostki w wymiarze co najmniej 4 godzin każda oraz co najmniej po 2 próby testów socjotechnicznych i penetracyjnych dla każdej jednostki.

Kody CPV

72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia
72222000-7 Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej oraz usługi w zakresie planowania
72222100-8 Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej
72223000-4 Usługi w zakresie wymogów technologii informacji
72224200-3 Usługi w zakresie planowania zapewniania jakości systemu
72240000-9 Usługi analizy systemu i programowania
72300000-8 Usługi w zakresie danych
72315000-6 Usługi zarządzania siecią danych oraz usługi wspierające
72316000-3 Usługi analizy danych
72810000-1 Usługi audytu komputerowego
80500000-9 Usługi szkoleniowe
80511000-9 Usługi szkolenia personelu

Miejsca realizacji

adres

Kraj
Polska

Województwo
dolnośląskie

Powiat
lwówecki

Gmina
Mirsk

Miejscowość
Mirsk

Harmonogram

Etap 1

Początek realizacji
2024-07-15

Koniec realizacji
2024-07-24

Opis
„Ankieta Dojrzałości Cyberbezpieczeństwa” do 24.07.2024r.

Czy występuje płatność częściowa

TAK

Etap 2

Początek realizacji

2024-07-15

Koniec realizacji

2026-03-31

Opis

Pozostałe części zamówienia zgodnie z przedstawionym przez Wykonawcę i Zaakceptowanym przez Zamawiającego harmonogramem jednak nie później niż do dnia 31.03.2026r.

Czy występuje płatność częściowa

TAK

Warunki, jakie musi spełniać oferent

Typ

Wiedza i doświadczenie

Opis

a. W okresie ostatnich 3 lat, zrealizował co najmniej cztery audyty cyberbezpieczeństwa (niewskazane w pkt. b, c, d) o wartości co najmniej 20 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzone referencjami;
b. Zrealizował co najmniej dwa inne audyty bezpieczeństwa informacji (niewskazane w pkt. a, c, d) o wartości co najmniej 10 000,00 zł brutto w podmiocie realizującym zadania publiczne, potwierdzony referencjami;
c. Wykonał co najmniej dwa projekty dotyczące szacowania ryzyka dla bezpieczeństwa danych w systemach informatycznych, potwierdzonych referencjami,
d. Wykonał co najmniej dwa projekty polegające na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów publicznych.
e. Posiada zespół składający się z co najmniej 2 osób, w tym:
 minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie audytowania systemów zarządzania bezpieczeństwem informacji przy spełnieniu wymagań dla audytorów IRCA, CQI

lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone certyfikatem ukończenia kursu Information Security Management Systems Auditor (ISMS) lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą aktualne uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
- minimum 1 osobą posiadającą kompetencje w zakresie audytowania systemów zarządzania ciągłością działania przy spełnieniu wymagań dla audytorów wiodących Systemu Zarzadzania Ciągłością Działania zgodnego z normą PN-EN ISO 22301 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla Audytora Wiodącego Systemu Zarzadzania Ciągłością Działania zgodnego z normą PN-EN ISO 22301 po zdaniu egzaminu lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą kompetencje w zakresie audytowania systemów zarządzania jakością przy spełnieniu wymagań dla audytorów wewnętrznych Systemu Zarzadzania Jakością zgodnego z normą PN-EN ISO 9001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla Audytora Wewnętrznego Systemu Zarzadzania Jakością zgodnego z normą PN-EN ISO 9001 po zdaniu egzaminu lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie wdrażania systemów zarządzania bezpieczeństwem informacji zgodnie z normą ISO 27001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem) oraz uczestniczącą w projektach wdrożenia systemu zarządzania bezpieczeństwem informacji na podstawie Rozporządzenia KRI w przynajmniej dwóch podmiotach publicznych;
- minimum 1 osobą posiadającą wiedzę i doświadczenie w zakresie ryzyka w ochronie informacji potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą, która uczestniczyła w co najmniej 2 projektach dotyczących zarządzania ryzykiem w bezpieczeństwie informacji, w tym w co najmniej 1 projekcie dotyczącym zarządzania ryzykiem na podstawie normy ISO 27005.
- minimum 1 osobą posiadającą wiedzę w zakresie wymagań Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą, która przeprowadziła co najmniej 10 szkoleń w zakresie cyberbezpieczeństwa / bezpieczeństwa informacji / ochrony danych dla podmiotów publicznych;
- minimum 1 osobą posiadającą wiedzę w zakresie zarządzania cyberbezpieczeństwem potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 1 osobą posiadającą wiedzę w zakresie administrowania sieciami teleinformatycznymi,

> potwierdzoną ważnym certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem).
> minimum 1 osobą, która odbyła specjalistyczne szkolenie w zakresie cyberbezpieczeństwa, na podstawie norm ISO 27001, 22301 i przepisów RODO, potwierdzone certyfikatem ukończenia szkolenia w tym zakresie lub innym równoważnym dokumentem (zaświadczeniem).

Kryteria oceny do części 1

Czy kryterium cenowe?

TAK

Opis

Cena 100%

Podsumowanie

Oś czasu związana z ogłoszeniem i ofertowaniem

-> 2024-07-09 - data opublikowania

-> 2024-07-12 11:00:00 - termin składania ofert

-> 2024-07 - planowany termin podpisania umowy

Oś czasu realizacji przedmiotów zamówienia

-> 2024-07-15 - Etap1 (początek): Usługa / Usługi inne / Zamówienie obejmuje dwa obszary działania w ramach realizacji zadania Cyberbezpieczna Gmina Mirsk. P...

2024-07-15 - Etap2 (początek): Usługa / Usługi inne / Zamówienie obejmuje dwa obszary działania w ramach realizacji zadania Cyberbezpieczna Gmina Mirsk. P...

-> 2024-07-24 - Etap1 (koniec): Usługa / Usługi inne / Zamówienie obejmuje dwa obszary działania w ramach realizacji zadania Cyberbezpieczna Gmina Mirsk. P... / występuje płatność częściowa

-> 2026-03-31 - Etap2 (koniec): Usługa / Usługi inne / Zamówienie obejmuje dwa obszary działania w ramach realizacji zadania Cyberbezpieczna Gmina Mirsk. P... / występuje płatność częściowa