Gmina Sępólno Krajeńskie planuje w najbliższym czasie przeprowadzić postępowanie o udzielenie zamówienia publicznego, którego przedmiotem będzie **Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji SZBI oraz przeprowadzenie Audytu Bezpieczeństwa Informacji dla Urzędu Miejskiego w Sępólnie Krajeńskim** w ramach projektu pn. „Poprawa Cyberbezpieczeństwa w Gminie Sępólno Krajeńskie", dofinansowanego w ramach programu grantowego „Cyberbezpieczny Samorząd" z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Przed wszczęciem postępowania obowiązkiem Zamawiającego jest oszacowanie wartości zamówienia. W celu poznania cen rynkowych tego zamówienia zwracamy się z prośbą o dokonanie wyceny przedmiotu zamówienia.

Opis przedmiotu zamówienia:

ZADANIE I: Przedmiotem zamówienia jest Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w tym: Polityka Bezpieczeństwa Informacji, Polityka ochrony danych osobowych, Polityka zarządzania systemem informatycznym, Polityka zarządzania ciągłością działania, Procedura zarządzania incydentami cyberbezpieczeństwa, Przeprowadzenie Analizy Ryzyka Systemu Zarządzania Bezpieczeństwem Informacji, Przygotowanie dokumentacji zgodnie z wymogami ustawy o KSC dla Urzędu Miejskiego w Sępólnie Krajeńskim

Zakres zadania:

W ramach realizacji przedmiotu zamówienia wykonawca opracuje dokumenty Systemu Zarządzania Bezpieczeństwem Informacji. Dokumentacja SZBI będzie wykonana w oparciu o:

- rozporządzenie Rady Ministrów z dnia 21 maja 2024 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773) (w zakresie dotyczącym bezpieczeństwa informacji),
- rozporządzenie 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),
- ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.).

Etapy realizacji usługi:

1) ***Etap I: „Polityka Bezpieczeństwa Informacji jako podstawowy element systemu zarządzania bezpieczeństwem informacji" obejmuje następujące czynności:***
   a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Bezpieczeństwa Informacji realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
   b) przygotowanie i przekazanie Polityki Bezpieczeństwa Informacji;
   c) doradztwo we wdrożeniu Polityki Bezpieczeństwa Informacji i bieżące wsparcie ekspertów przez czas trwania Umowy;

2) ***Etap II: „Polityka Zarządzania Systemem Teleinformatycznym" obejmuje następujące czynności:***
   a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Systemem Informatycznym realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
   b) przygotowanie i przekazanie Polityki Zarządzania Systemem Informatycznym wraz z Planami Ciągłości Działania w obszarze IT;
   c) doradztwo we wdrożeniu Polityki Zarządzania Systemem Informatycznym i bieżące wsparcie ekspertów przez czas trwania Umowy;

3) ***Etap III: „Polityka Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT" obejmuje następujące czynności:***
   a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Ciągłością Działania realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
   b) przygotowanie i przekazanie Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT;
   c) doradztwo we wdrożeniu Polityki Zarządzania Ciągłością Działania i bieżące wsparcie ekspertów przez czas trwania Umowy;

4) ***Etap IV: „Polityka Zarządzania Incydentami Cyberbezpieczeństwa" obejmuje następujące czynności:***
   a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Incydentami Cyberbezpieczeństwa realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
   b) przygotowanie i przekazanie Polityki Zarządzania Incydentami Cyberbezpieczeństwa;

c) przygotowanie i przekazanie Planu Reagowania na Incydenty;
d) przygotowanie i przekazanie Planu Zarządzania Podatnościami;
e) doradztwo we wdrożeniu dokumentacji i bieżące wsparcie ekspertów przez czas trwania Umowy;

5) ***Etap V: „Polityka Ochrony Danych" obejmuje następujące czynności:***
a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Ochrony Danych realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
b) przygotowanie i przekazanie Polityki Ochrony Danych;
c) doradztwo we wdrożeniu Polityki Ochrony Danych i bieżące wsparcie ekspertów przez czas trwania Umowy;

6) ***Etap VI: „Analiza Ryzyka Bezpieczeństwa Informacji" obejmuje następujące czynności:***
a) konsultacje z przedstawicielem Zamawiającego w celu przeprowadzenia analizy ryzyka realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
b) przygotowanie i przekazanie Raportu z przeprowadzonej analizy ryzyka wraz z omówieniem obszarów o podniesionym ryzyku wraz z rekomendacjami ekspertów.

7) ***Etap VII: W ramach realizowanej usługi, ponad czynności o których mowa w pkt 1-6, zostaną przygotowane przez Wykonawcę lub dostosowane w przypadku ich posiadania przez Zamawiającego, następujące dokumenty:***
a) procedury korzystania z urządzeń mobilnych,
b) procedury pracy zdalnej,
c) postępowanie z nośnikami,
d) procedury kontroli dostępu,
e) zabezpieczenie pomieszczeń i obiektów,
f) procedury czystego biurka,
g) procedury czystego ekranu,
h) procedury kopii zapasowych,
i) procedury ochrony logów,
j) bezpieczeństwo komunikacji,
k) zarządzanie bezpieczeństwem sieci,
l) przesyłanie informacji,
m) plany ciągłości działania,

n) procedury zarządzania incydentami,
o) prywatność i ochrona danych osobowych,
p) szacowanie ryzyka w obszarze bezpieczeństwa informacji,
q) szkolenia personelu,
r) plan zarządzania podatnościami,
s) plan reagowania na incydenty,
t) plan przywracania.

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami oraz wszelkich innych informacji uzyskanych w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji.

ZADANIE II: Przedmiotem zamówienia jest Przeprowadzenie Audytu Bezpieczeństwa Informacji zgodnego z przepisami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 roku w sprawie Krajowych Ram Interoperacyjności oraz końcowej ankiety dojrzałości cyberbezpieczeństwa dla Urzędu Miejskiego w Sępólnie Krajeńskim **oraz jednostek podległych tj. Centrum Usług Społecznych; Centrum Małego Dziecka i Rodziny; Centrum Sportu i Rekreacji**

Zakres zadania:

1) weryfikacja zgodności przyjętych procedur z przepisami 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 (t. j. Dz. U. 2024 r., poz. 773);
2) weryfikacja zgodności przyjętych procedur z zakresu cyberbezpieczeństwa wynikających z obowiązków określonych w przepisach Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.));
3) weryfikacja zgodności przyjętych procedur z przepisami z zakresu ochrony danych wynikających z obowiązków określonych w przepisach 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 Dz. U. UE. L. 2016, poz. 119.1 i 2. – dalej „RODO") oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781);
4) testy podatności infrastruktury teleinformatycznej;
5) audyt infrastruktury sieciowej;
6) przygotowanie i przekazanie raportu z Audytu końcowego;

7) omówienie wyników Audytu końcowego oraz wydanie rekomendacji Zamawiającemu

8) Przeprowadzenie ankiety dojrzałości cyberbezpieczeństwa w oparciu o załącznik nr. 6 umieszczony na stronie https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

Ofertę cenową należy przesłać **do dnia 08.05.2026 r. do godziny 12:00** na adres e-mail: **zamowienia@gmina-sepolno.pl**.

Oferty prosimy przesyłać według poniższej formuły.

ZADANIE I

Wartość netto: .....PLN

VAT..... % .....PLN

Cena brutto:.....PLN

ZADANIE II

Wartość netto: .....PLN

VAT..... % .....PLN

Cena brutto:.....PLN

Osoby upoważnione do kontaktu z Wykonawcami: Jolanta Tryk.

Tel.: /052/ 389 42 52

Uwaga: Udział Wykonawców w rozeznaniu rynku oraz złożone propozycje cenowe nie będą stanowić podstawy do udzielenia zamówienia któremukolwiek z Wykonawców.

Załączniki:

1) Klauzula RODO

Z up. BURMISTRZA

mgr Anna Sotkiewicz-Tumanik

Kierownik Referatu Inwestycji i Rozwoju Gospodarczego