Cyberbezpieczny Samorząd

Załącznik nr 3 do Regulaminu udzielania przez Gminę Nowa Ruda zamówień publicznych, których wartość nie przekracza kwoty 130.000 złotych

Nr sprawy: **OSOOC.271.7.2025**

Nowa Ruda, dnia 18.02.2025 r.

Gmina Nowa Ruda
ul. Niepodległości 2
57-400 Nowa Ruda
NIP: 8851534651
(pełna nazwa Zamawiającego – nazwa, adres, NIP, REGON, adres e-mail)

ZAPROSZENIE

DO ZŁOŻENIA OFERTY NA REALIZACJĘ ZAMÓWIENIA PN.:

1.a. Usługa opracowania dokumentacji oraz wdrożenie normy **PN-EN ISO/IEC 27001:2023-08** Systemu Zarządzania Bezpieczeństwem Informacji dla Zamawiającego, zgodnie z warunkami określonymi w § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".
1.b. Przeprowadzenie szkolenia dla zespołu wdrożeniowego SZBI Zamawiającego,
1.c. Wsparcie merytoryczne zespołu wdrożeniowego SZBI Zamawiającego;

2. usługa opracowania szacowania ryzyka zgodnie z § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".

W związku z realizacją zadań związanych z

Projektem w ramach FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Projekt realizowany jest przez Centrum Projektów Polska Cyfrowa (Beneficjent Projektu) w Partnerstwie z NASK Państwowym Instytutem Badawczym.

Opis przedmiotu zamówienia:

1.a. Usługa opracowania dokumentacji **oraz wdrożenie normy PN-EN ISO/IEC 27001:2023-08** Systemu Zarządzania Bezpieczeństwem Informacji dla Zamawiającego, zgodnie z warunkami określonymi w § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".
1.b. Przeprowadzenie szkolenia dla zespołu wdrożeniowego SZBI Zamawiającego,
1.c. Wsparcie merytoryczne zespołu wdrożeniowego SZBI Zamawiającego;

2. usługa opracowania szacowania ryzyka zgodnie z § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".

Ad1.a. Dokumentacja musi obejmować bezpieczeństwo **fizyczne (**ochrona pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), **bezpieczeństwo informatyczne** (bezpieczeństwo systemu teleinformatycznego) oraz **bezpieczeństwo osobowe i organizacyjne (stosowane procedury bezpieczeństwa).**

Dokumentacja musi obejmować następujące obszary:

a. ustanowienie polityki bezpieczeństwa informacji oraz polityk tematycznych,
b. aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji,
c. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
d. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
e. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia,
f. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji,
g. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
h. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
i. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
j. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,

k. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,

l. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,

m. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,

n. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- *Rozporządzenie 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 (zwanym dalej „Rozporządzeniem KRI");*
- 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.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:

- Kompleksowej dokumentacji systemu zarządzania bezpieczeństwem informacji,
- rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.

1.b. W ramach usługi Wykonawca przeprowadzi szkolenie zespołu wdrożeniowego Zamawiającego w zakresie systemu zarządzania bezpieczeństwem informacji.

1.c. W ramach usługi Zamawiający zapewni wsparcie zespołu wdrożeniowego SZBI Zamawiającego, które odbywać się będzie w formie konsultacji, od poniedziałku do piątku, realizowanych w trakcie wdrożenia, poprzez bezpieczne formy komunikacji, takie jak: rozmowa telefoniczna, poczta e-mail, telekonferencja lub stacjonarnie w siedzibie Zamawiającego.

2. Szacowanie ryzyka musi obejmować bezpieczeństwo **fizyczne (**ochrona pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), **bezpieczeństwo informatyczne** (bezpieczeństwo systemu teleinformatycznego) oraz **bezpieczeństwo osobowe i organizacyjne (stosowane procedury bezpieczeństwa).**

Szacowanie ryzyka musi obejmować własności bezpieczeństwa informacji:

- dostępność - jest to właściwość określającą, że zasób jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony,
- integralności - jest to właściwość określającą, że zasób nie został zmodyfikowany w sposób nieuprawniony,
- poufności - jest to właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym.

Szacowanie Ryzyka musi obejmować następujące etapy:

a) Analizę ryzyka:
- identyfikacja aktywów, czyli informacje, osoby, usługi, oprogramowanie, dane i sprzęt, a także inne elementy mające wpływ na bezpieczeństwo informacji
- identyfikacja zagrożeń, czyli niepożądane zdarzenia, mogące mieć wpływ na dane osobowe
- identyfikacja podatności, czyli słabość zasobu lub zabezpieczenia , która może zostać wykorzystana przez zagrożenie
- identyfikacja zabezpieczeń, czyli środki o charakterze fizycznym, technicznym lub organizacyjnym
- identyfikacja skutków, czyli wyników działania zagrożenia
- określenie wielkości ryzyk, czyli wyznacza się poziomy zidentyfikowanych ryzyk

b) Ocenę ryzyka:
- Porównanie wyznaczonych poziomów ryzyk z tymi, które można zaakceptować – postępowanie z ryzykiem

Szacowanie Ryzyka musi zostać wykonane zgodnie z normą ISO/IEC 27005.

Szacowanie musi uwzględniać wymagania następujących aktów prawnych oraz norm:
- *Rozporządzenie 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;*
- *Ustawa o Krajowym Systemie Cyberbezpieczeństwa;*
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023;
- Norma ISO/IEC 27005:2022;
- Norma PN-EN ISO/IEC 22301:2020.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:
- Kompleksowej dokumentacji wykonanego szacowania ryzyka wraz z raportem,
- rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.

1. **Wymagany termin realizacji przedmiotu zamówienia:**
   1.a. Usługa opracowania dokumentacji **oraz wdrożenie normy PN-EN ISO/IEC 27001:2023-08** Systemu Zarządzania Bezpieczeństwem Informacji dla Zamawiającego, zgodnie z warunkami określonymi w § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".
   1.b. Przeprowadzenie szkolenia dla zespołu wdrożeniowego SZBI Zamawiającego,
   1.c. Wsparcie merytoryczne zespołu wdrożeniowego SZBI Zamawiającego;

2. usługa opracowania szacowania ryzyka zgodnie z § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".

musi być wykonany do dnia 31 maja 2025 r.

2. Informacja, czy zamówienie jest dofinansowane ze środków Unii Europejskiej*: TAK/~~NIE~~

3. **Przy wyborze oferty do realizacji, Zamawiający będzie kierował się następującymi kryteriami:** (cena – 100 % - jeżeli będą miały zastosowanie inne kryteria , to należy je podać)

4. **Wykonawca składając ofertę zobowiązany jest złożyć następujące dokumenty:**
   1) formularz oferty wg załączonego wzoru – **Załącznik nr 4**,

   2) oświadczenie Wykonawcy, że spełnia następujące warunki udziału w postępowaniu:

- Wykonawca należycie wykonał co najmniej 2 usługi przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla podmiotów realizujących zadania publiczne, z których każda miała wartość nie mniejszą niż 15 000,00 zł netto, co zostało udokumentowane referencjami;
- W okresie ostatnich 4 lat, zrealizował co najmniej 8 audytów bezpieczeństwa informacji o wartości co najmniej 15 000,00 zł netto w podmiocie realizującym zadania publiczne, potwierdzony referencjami;
- Wykonał co najmniej trzy projekty dotyczące szacowania ryzyka dla bezpieczeństwa danych w systemach informatycznych, potwierdzonych referencjami,
- Wykonał co najmniej trzy projekty polegające na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów publicznych.

Posiada zespół składający się z co najmniej 3 osób, w tym:

- minimum 2 osobami posiadającymi 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, potwierdzonych zaświadczeniem ukończenia kursu Information Security Management Systems (ISMS) Auditor lub innym równoważnym dokumentem;
- minimum 2 osobami posiadającymi 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 2 osobami posiadającymi 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 2 osobami posiadającymi wiedzę i doświadczenie w zakresie ochrony danych osobowych potwierdzone dyplomem ukończenia studiów podyplomowych w zakresie ochrony danych osobowych oraz posiadającymi co najmniej 8 letnie doświadczenie w pełnieniu funkcji Inspektora Ochrony Danych / Administratora Bezpieczeństwa Informacji;
- 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 2 osobami, które uczestniczyły 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 ukończyła wyższe studia techniczne w zakresie cyberbezpieczeństwa oraz uzyskała tytuł inżyniera, potwierdzony dyplomem ukończenia studiów wyższych.
- 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).

Do oferty i oświadczenia, o którym mowa w lit. 2, należy dołączyć:

3) Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej 2 usług przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla podmiotów realizujących zadania publiczne, z których każda miała wartość nie mniejszą niż 15 000,00 zł netto;
4) Referencje lub inny dokument potwierdzający prawidłowe wykonanie, w okresie ostatnich 4 lat, co najmniej 8 audytów bezpieczeństwa informacji o wartości co najmniej 15 000,00 zł netto w podmiocie realizującym zadania publiczne, potwierdzony referencjami;
5) Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej trzech projektów dotyczących szacowania ryzyka dla bezpieczeństwa danych w systemach informatycznych, w tym w co najmniej 1 projekcie dotyczącym zarządzania ryzykiem na podstawie normy ISO 27005;
6) Referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej trzech projektów polegających na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów publicznych;
7) Co najmniej dwa zaświadczenia ukończenia kursu Information Security Management Systems Auditor (ISMS);
8) Co najmniej 2 aktualne certyfikaty wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
9) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301;
10) Co najmniej 2 certyfikaty Audytora Wewnętrznego Systemu Zarządzania Jakością według normy PN-EN ISO 9001;
11) Dyplomy ukończenia studiów podyplomowych w zakresie ochrony danych osobowych / bezpieczeństwa informacji;
12) Referencje lub inne dokumenty potwierdzające odpowiednie doświadczenie (co najmniej 8 lat) na stanowisku związanym z ochroną danych osobowych/ bezpieczeństwem informacji;
13) Certyfikat/ zaświadczenie ukończenia szkolenia w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji wg ISO 27001;
14) Certyfikat/ zaświadczenie ukończenia szkolenia w zakresie ryzyka w ochronie informacji;
15) Certyfikat ukończenia szkolenia w zakresie wymagań Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
16) Referencje za przeprowadzenie co najmniej 10 szkoleń w zakresie cyberbezpieczeństwa / bezpieczeństwa informacji / ochrony danych dla podmiotów publicznych;
17) Certyfikat ukończenie szkolenia w zakresie zarządzania cyberbezpieczeństwem;

18) Certyfikat ukończenia szkolenia w zakresie administrowania sieciami teleinformatycznymi;
19) Dyplom ukończenia wyższych studiów technicznych w zakresie cyberbezpieczeństwa, potwierdzający uzyskanie tytułu inżyniera;
20) Zaświadczenie o odbyciu specjalistycznego szkolenia w zakresie cyberbezpieczeństwa na podstawie norm ISO 27001, 22301 i przepisów RODO;

5. **Opis sposobu obliczenia ceny w składanej ofercie:**
Cena powinna zawierać:
1) ~~wartość dostawy~~* /usługi*/~~roboty budowlanej~~* określoną w oparciu o przedmiot zamówienia,
2) obowiązujący podatek od towarów i usług VAT.

6. **Zamawiający wybierze ofertę z najkorzystniejszą ceną oraz spełniającą wszystkie wymagane warunki.**

7. **Opis sposobu przygotowania oferty:**
1) Ofertę należy złożyć w nieprzejrzystej i zamkniętej kopercie z dopiskiem: „Oferta na zadanie pn. ……." bezpośrednio w siedzibie Zamawiającego lub przesłać e-mailem na adres: sekrtariat@gmina.nowaruda.pl*.

Cena podana w złożonej ofercie ma być podana cyfrowo i słownie. Oferta cenowa winna być sporządzona wyłącznie w języku polskim i musi obejmować całość zamówienia. Formularz składany drogą pocztową należy wypełnić czytelną i trwałą techniką. W przypadku oferty składanej drogą elektroniczną powinna być ona przygotowana w formacie uniemożliwiającym edycję (np. pdf).*

8. **Miejsce i termin złożenia oferty :**
1) Ofertę należy złożyć w terminie do dnia 28 lutego 2025 r., do godz. 10:00 w siedzibie Zamawiającego (57-400 Nowa Ruda, ul. Niepodległości 2) lub wysyłając na adres mailowy: sekretariat@gmina.nowaruda.pl*.
2) Oferta otrzymana przez Zamawiającego po terminie podanym w zaproszeniu nie będzie brana pod uwagę, a dodatkowo – oferta złożona drogą pocztową zostanie Wykonawcy zwrócona bez otwierania.

9. **Miejsce i termin otwarcia oferty:**
Otwarcie złożonych ofert nastąpi w dniu 28 lutego 2025 r., o godz. 11:00 w siedzibie Zamawiającego.

10. **Osobami uprawnionymi do kontaktów z Wykonawcami są** :

Piotr Brzóska
Główny Specjalista ds. Informatycznych
Referat Organizacyjny, Spraw Obywatelskich i Zarządzania Kryzysowego

Tel. (74) 872 54 69
email: p_brz@gmina.nowaruda.pl

(imię i nazwisko, nr telefonu, adres mailowy)

11. **Informacje dotyczące zawierania umowy.**
Umowa musi zawierać wszystkie uwarunkowania złożonej propozycji cenowej.*

Nowa Ruda, dnia 18.02.2025 r.

Zastępca Wójta
Anna Zawiślak

.....
(data i podpis Zamawiającego)

* niepotrzebne skreślić/wpisywać, jeżeli dotyczy