Cyberbezpieczny Samorząd

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

Nr sprawy: **OSOZK.271.31.2025**

Nowa Ruda, dnia 12.11.2025 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.:

Usługa:

a. **Usługa Przeprowadzenia audytu zgodności z KRI, którego kryterium jest *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")"* zgodnie z § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd". Audyt należy przeprowadzić do końca 2025 r.**
b. **Usługa polegająca na przeprowadzeniu szkoleń z zakresu cyberbezpieczeństwa. Szkolenia muszą być zrealizowane w siedzibie Zamawiającego.**
c. **Usługa polegająca na przeprowadzeniu Testów socjotechnicznych pracowników Zamawiającego.**
d. **Usługa polegająca na przeprowadzeniu Testów podatnościowych systemu teleinformatycznego Zamawiającego. Testy muszą być zrealizowane w siedzibie Zamawiającego.**

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:

Ad. a. Usługa Przeprowadzenia audytu zgodności z KRI w początkowej fazie realizacji projektu, którego kryterium jest *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")"* zgodnie z § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd"

Audyt musi być przeprowadzony przez:

- 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~~ 4 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;

Audyt musi być zrealizowany w siedzibie Zamawiającego, w wymiarze co najmniej 1 dnia roboczego (tj. 8 godzin) do dna 31 grudnia 2025 r.

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) oraz bezpieczeństwa organizacyjnego i osobowego (stosowane procedury bezpieczeństwa), w tym przegląd dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji.

Audyt musi obejmować weryfikację:

a. systemu zarządzania bezpieczeństwem informacji,
b. zapewnienia 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.

Kryteriami audytu są:

- *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 ISO/IEC 27001;
- Norma PN-EN ISO/IEC 22301.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:

- raportu z audytu bezpieczeństwa systemu informacyjnego,
- rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.

Ad. b. Usługa: „przeprowadzenia szkoleń w zakresie cyberbezpieczeństwa skierowanych do osób zatrudnionych u Zamawiającego w zakresie ataków cybernetycznych oraz metod obrony przed tymi atakami"

Przedmiotem zamówienia jest usługa wykonania szkoleń, zgodnie z wymogiem § 90 ust. 6 *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;.*

I. Opis przedmiotu zamówienia:

1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa.

Szkolenia muszą być zrealizowane w siedzibie Zamawiającego.

W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni. Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trenerzy muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny.

Szkolenie ma zapoznać uczestnika z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem.

Uczestnicy mają dowiedzieć się jak działa rynek cyberprzestępczy, jakimi kwotami operują współcześni przestępcy, jakimi sposobami próbują uzyskać dostęp do sieci teleinformatycznej oraz jak w czasie rozmowy osobistej, telefonicznej lub mailowej oszuści potrafią wyłudzić informację od nieświadomego pracownika. Podczas szkolenia uczestnik ma być również edukowany ze skutków, dla których wykorzystywanie komputera służbowego do celów prywatnych zwiększa ryzyko ataku na całą organizację.

Szkolenie musi być skierowane do każdego pracownika w organizacji bez względu na jego wiedzę i umiejętności informatyczne.

Korzyści po szkoleniu:

- zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi
- zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi

Wykonawca zobowiązany jest do:

- wydania imiennych zaświadczeń / certyfikatów dla każdego uczestnika,
- zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej.

II. Szczegółowy wykaz szkoleń:

a) Szkolenie - podstawy cyberbezpieczeństwa dla pracowników (wymiar szkolenia: 2 h na turę), o następującej tematyce:

- Co to jest cyberprzestępczość?
- Opis funkcjonowania zorganizowanych grup cyberprzestępczych
- Czy jestem atrakcyjnym „klientem" dla cyberprzestępcy?
- Jakie zyski może mieć cyberprzestępca atakując moje dane?
- Straty wynikające z udanego ataku
- Rodzaje ataków skierowane w użytkowników Internetu
- Jak bronić się przed cyberprzestępcami?
- Spam jako niegroźny sposób na groźne ataki
- Handel adresami e-mail
- Kampanie Phishingowe
- Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję
- Groźne ataki 0-day
- Nieopłacona FV jako sposób przemycenia wirusa do naszego komputera
- Ataki socjotechniczne - czyli niewinne „wyłudzanie" danych
- Przekazywanie haseł dostępowych znajomym
- Fizyczne bezpieczeństwo danych osobowych
- Znaleziony pendrive na parkingu jako pozwolenie na atak dla cyberprzestępcy
- Aktualne zagrożenia wynikające z wojny w Ukrainie
- Podsumowanie szkolenia, pytania, dyskusja

Ad. C. Usługa: „wykonania testów socjotechnicznych wobec pracowników Zamawiającego"

Przedmiotem zamówienia jest usługa wykonania prób ataków socjotechnicznych za pomocą poczty e-mail.

I. Opis przedmiotu zamówienia:

2. Przedmiotem zamówienia jest przeprowadzenie „Testów socjotechnicznych pracowników Zamawiającego";

Testy muszą być zrealizowane w wymiarze co najmniej 7 dni roboczych (tj. 16 godzin).

Przeprowadzenie prób ataków socjotechnicznych polega na wywieraniu wpływu na ludzi i stosowaniu perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji. Przeprowadzane próby w Organizacji miały na celu zweryfikowanie świadomości pracowników i zabezpieczeń przed atakami socjotechnicznymi.

Testy muszą składać się z następujących faz:

1. Rozpoznanie (biały wywiad, obserwacja pracy pracowników).
2. Budowanie więzi i zaufania (użycie wewnętrznych informacji, podawanie się za kogoś innego, wspominanie nazwisk osób znanych ofierze, zgłoszenie potrzeby pomocy lub zasugerowanie posiadania władzy).
3. Wykorzystanie zaufania (prośba o informację lub działanie skierowana do ofiary).

Testy muszą być przeprowadzone za pomocą aktualnych narzędzi, wykorzystujących najnowsze możliwości w zakresie symulacji złośliwych kampanii socjotechnicznych.

Zakres testów:

Próba wyrywkowego przeprowadzenia testów socjotechnicznych za pomocą e-maila - próba będzie polegała na wysłaniu wiadomości e-mail na adresy służbowe pracowników Organizacji i przeprowadzeniu ataku socjotechnicznego.

Przygotowane przez testerów wiadomości muszą odpowiadać realnym atakom, realizowanym aktualnie przez przestępców. Wykonawca musi uwzględnić:

- Ataki typu phishing,
- Ataki typu spear phishing
- Phishing typu whaling
- Phishing przez klonowanie

- Angler phishing

Wykonawca zobowiązany jest do wykrycia (w stosunku do konkretnego adresu email):

- otwieranych wiadomości,
- otwieranych stron za pomocą linków umieszczonych w wiadomościach,
- podawanych poświadczeń na stronach mających na celu wyłudzanie informacji, przygotowanych przez testerów,
- pobieranie plików w popularnych formatach, takich jak „docx.", czy „xlsx",
- otwierania plików w popularnych formatach, takich jak „docx.", czy „xlsx".

Ad. d. Usługa: „wykonania testów podatnościowych infrastruktury teleinformatycznej"

Przedmiotem zamówienia jest usługa wykonania testów podatnościowych, zgodnie z wymogiem § 19 ust 12 lit. f oraz g *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;.*

Opis przedmiotu zamówienia:

3. Przedmiotem zamówienia jest przeprowadzenie „Testów podatnościowych systemu teleinformatycznego Zamawiającego";

Testy muszą być zrealizowane w siedzibie Zamawiającego, w wymiarze co najmniej 2 dni roboczych (tj. 16 godzin).

Celem przeprowadzenia testów podatności systemu teleinformatycznego ma być zidentyfikowanie słabych punktów bezpieczeństwa, opierając się na zidentyfikowanych podatnościach.

Testy muszą obejmować hosty w sieci wewnętrznej oraz dostępne z poziomu sieci publicznej, w wyznaczonych adresacjach. Dodatkowo Wykonawca musi przeprowadzić analizę topologii sieci wraz z próbami wykrycia nieszczelności w skonfigurowanych urządzeniach.

Testy muszą składać się z następujących faz:

a. Faza rozpoznania - rozpoznanie aktywne - obejmuje działania mające na celu zebranie informacji o testowanym systemie. Aktywność testującego opiera się na bezpośredniej interakcji ze środowiskiem celu. Zawiera w sobie działania takie jak skanowanie portów, wykrywanie usług, czy hostów działających w sieci.
b. Faza oceny podatności sieci wewnętrznej oraz urządzeń dostępnych z poziomu sieci Internet - analiza występowania w badanym systemie podatności zawartych w bazach danych podatności takich jak National Vulnerability Database (NVD), czy Common Vulnerabilities and Exposures (CVE); ocena wykorzystania skompromitowanych

protokołów; weryfikacja słabości systemu na popularne ataki takie jak Man-in-the-middle attack, Denial-of-service attack, Brute Force czy SQL injection.

c. Próby exploitacji wykrytych podatności technicznych;
d. Przygotowanie raportu z oceny wraz z zaleceniami działań naprawczych.

Testy muszą być przeprowadzone przez aktualne narzędzia, wykorzystujące najnowsze bazy podatności.

Zakres testów:

a) testy bezpieczeństwa sieci teleinformatycznych, w tym brzegu sieci;
b) testy bezpieczeństwa baz danych;
c) testy bezpieczeństwa środowisk serwerowych, w tym systemów operacyjnych;
d) testy bezpieczeństwa środowisk wirtualnych;
e) Konsultacje dot. prezentacji metod wykorzystania znalezionych podatności i propozycji sposobów wdrożenia zabezpieczeń teleinformatycznych.

Wykonawca zobowiązany jest do:

- wykrycia działających usług w systemach Zamawiającego,
- wykrycia otwartych portów na poszczególnych urządzeniach,
- zidentyfikowania podatności na poszczególnych hostach,
- wyszukania błędów konfiguracyjnych, które skutkowały powstaniem określonych luk w zabezpieczeniach,
- określenia stopnia istotności wyszukanych podatności technicznych,
- opracowania raportu podsumowującego z zaleceniami działań naprawczych.

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

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

3. **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 6 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 3 osoby 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;

4. **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.

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

6. **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).*

7. **Miejsce i termin złożenia oferty :**
   1) Ofertę należy złożyć w terminie do dnia 1 grudnia 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.

8. **Miejsce i termin otwarcia oferty:**
Otwarcie złożonych ofert nastąpi w dniu 1 grudnia 2025 r., o godz. 11:00 w siedzibie Zamawiającego.

9. **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)

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

Nowa Ruda, dnia 12.11.2025 r.

Zastępca Wójta
Anna Zawiślak
……
(data i podpis

Zamawiającego)

* niepotrzebne skreślić/wpisywać, jeżeli dotyczy