Nowy Duninów, 15.06.2026 r.

Zapytanie ofertowe nr IGK.2600.57.06.2026.RW

W postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie zapytania ofertowego o wartości poniżej kwoty określonej w art.2 ust.1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

Zamawiający: Gmina Nowy Duninów

ul. Osiedlowa 1

09 – 505 Nowy Duninów

Zaprasza do złożenia ofert cenowych w ramach postępowania:

Szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy w Nowym Duninowie w ramach projektu „Cyberbezpieczny Samorząd"

I. Warunki formalno – prawne zapytania ofertowego.

1. Przedmiotowe zapytanie ofertowe prowadzone jest z wyłączeniem stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz. U. z 2024 r. poz. 1320 ze zm.) na podstawie art. 2 ust 1. pkt 1 tejże ustawy.
2. Zamawiający wybierze ofertę uznaną za najkorzystniejszą spośród prawidłowo złożonych ofert przez Wykonawców spełniających warunki udziału w postępowaniu.
3. Zamawiający odrzuci oferty z rażąco niską ceną w stosunku do przedmiotu zamówienia oraz budzące wątpliwości co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w treści zapytania ofertowego.
4. Zamawiający zastrzega sobie prawo do podjęcia z Wykonawcami negocjacji cen ofertowych w celu ulepszenia treści ofert lub w przypadku, gdy cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający może przeznaczyć na realizację zamówienia.
5. Zamawiający zastrzega sobie prawo do unieważnienia postępowania na każdym jego etapie bez podania przyczyny.

6. Zamawiający informuje o konieczności publikacji danych z formularza ofertowego. Niezbędne dane to nazwa albo imię i nazwisko Wykonawcy, adres prowadzenia działalności gospodarczej albo adres zamieszkania w przypadku osoby fizycznej oraz cena oferty. Publikacja tych danych osobowych jest konieczna ze względu na realizację podstawowego celu zasady konkurencyjności: transparentność (przejrzystość) oraz równe traktowanie Wykonawców.

7. Wykonawca składając ofertę oświadcza, że nie podlega wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego. Zamawiający odrzuci ofertę Wykonawcy, która podlega wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

II. Przedmiot zamówienia: „Szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy w Nowym Duninowie w ramach projektu „Cyberbezpieczny Samorząd".

1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy w Nowym Duninowie, realizowanych w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd" w Programie Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC), Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

2. Zamówienie obejmuje wykonanie szkoleń dla pracowników w celu podniesienia świadomości w zakresie cyberzagrożeń, ochrony danych oraz bezpiecznego korzystania z systemów teleinformatycznych wykorzystywanych w działalności jednostki samorządu terytorialnego.

III. Zakres szkolenia

1. Szkolenie należy przeprowadzić w formie stacjonarnej.
2. Liczba uczestników: 30 osób.
3. Szkolenie powinno obejmować minimum 16 godzin dydaktycznych.
4. Miejscem realizacji szkolenia będzie siedziba Urzędu Gminy w Nowym Duninowie lub inne miejsce wskazane przez Zamawiającego na terenie gminy.
5. Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników.
6. Po zakończeniu szkolenia Wykonawca przekaże uczestnikom zaświadczenia lub certyfikaty potwierdzające udział w szkoleniu. Dokument potwierdzający udział powinien zawierać co najmniej: imię i nazwisko uczestnika, nazwę szkolenia, datę realizacji oraz dane Wykonawcy.

7. Zakres tematyczny szkolenia obejmuje co najmniej:
1) Wprowadzenie do cyberbezpieczeństwa w sektorze publicznym:
a) Znaczenie cyberbezpieczeństwa w instytucjach państwowych,
b) Przegląd obowiązujących przepisów i standardów, w tym kluczowych elementów dyrektywy NIS2,
c) Potencjalne zagrożenia cybernetyczne i ich skutki dla sektora publicznego oraz obywateli.
2) Podstawowe pojęcia i terminologia NIS2:
a) Kluczowe definicje: kluczowa infrastruktura, incydent, system informatyczny, wskaźniki KRI,
b) Wymagania dyrektywy NIS2 w kontekście ochrony zasobów państwowych i danych obywateli,
c) Rola instytucji państwowych w ochronie infrastruktury krytycznej.
3) Rozpoznawanie i zarządzanie ryzykiem (KRI i analiza ryzyka):
a) Przegląd metod oceny ryzyka i wdrażanie kluczowych wskaźników ryzyka (KRI),
b) Dokumentowanie i monitorowanie ryzyk: katalog ryzyk i procedury oceny ryzyka,
c) Omówienie scenariuszy ryzyka oraz metod ich łagodzenia w kontekście NIS2.
4) Bezpieczeństwo systemów informatycznych w instytucjach państwowych:
a) Zasady bezpiecznego logowania i zarządzania dostępem do systemów (m.in. MFA, silne hasła),
b) Znaczenie regularnych aktualizacji i stosowanie narzędzi antywirusowych oraz firewalli,
c) Zasady segmentacji sieci oraz ochrona przed nieautoryzowanym dostępem.
5) Ochrona danych osobowych i wrażliwych zgodnie z NIS2 i RODO:
a) Podstawowe zasady przetwarzania i ochrony danych osobowych w instytucjach publicznych,
b) Polityki ochrony danych i wymagania dotyczące ochrony infrastruktury krytycznej,
c) Zasady raportowania naruszeń ochrony danych osobowych i reagowania na incydenty.
6) Ochrona przed phishingiem, socjotechniką i wewnętrznymi zagrożeniami:
a) Identyfikacja zagrożeń phishingowych oraz ich rozpoznawanie,
b) Techniki socjotechniczne i sposoby ich przeciwdziałania,
c) Zarządzanie dostępem oraz metody ograniczania ryzyka ze strony pracowników i osób trzecich.
7) Bezpieczne korzystanie z sieci wewnętrznych i zasobów publicznych:
a) Zasady bezpieczeństwa sieci wewnętrznych: zabezpieczenia, monitoring i kontrola dostępu,
b) Stosowanie certyfikatów i szyfrowania przy połączeniach z siecią zewnętrzną,
c) Bezpieczne korzystanie z urządzeń mobilnych oraz VPN w pracy zdalnej.
8) Procedury zarządzania incydentami i zgłaszania incydentów (zgodnie z NIS2):

a) Definicja incydentu oraz procedury postępowania w przypadku jego wystąpienia,
b) Ścieżka zgłaszania incydentów do odpowiednich organów (np. CSIRT),
c) Wskaźniki SLA oraz RTO/RPO w raportowaniu incydentów, a także obowiązki instytucji zgodnie z NIS2.
9) Ochrona fizyczna oraz ochrona nośników danych:
a) Fizyczne zabezpieczenie sprzętu, systemów i nośników danych,
b) Zasady przechowywania, szyfrowania i bezpiecznego niszczenia danych,
c) Zasady i środki ochrony infrastruktury krytycznej zgodne z dyrektywą NIS2.

IV. Zakres obowiązków Wykonawcy

Wykonawca zobowiązany będzie do:

1. Opracowania programu szkolenia zgodnego z wymaganiami Zamawiającego.
2. Przeprowadzenia szkolenia przez osoby posiadające odpowiednie kwalifikacje i doświadczenie.
3. Przygotowania oraz przekazania materiałów szkoleniowych uczestnikom.
4. Przeprowadzenia list obecności uczestników.
5. Wydania uczestnikom dokumentów potwierdzających ukończenie szkolenia.
6. Przekazania Zamawiającemu dokumentacji potwierdzającej realizację szkolenia, w szczególności list obecności i kopii wydanych zaświadczeń lub certyfikatów.

V. Warunki realizacji zamówienia

1. Wynagrodzenie za realizację zadania zostanie wypłacone Wykonawcy na podstawie prawidłowo wystawionej faktury po wykonaniu całości przedmiotu zamówienia.
2. Termin związania ofertą – 30 dni od dnia upływu terminu składania ofert.
3. Kod CPV: 80511000-9 – Usługi szkolenia personelu.
4. Zamawiający nie dopuszcza składania ofert częściowych.
5. Zamawiający dopuszcza realizację przedmiotu zamówienia z udziałem podwykonawców. Wykonawca odpowiada za działania podwykonawców jak za własne.
6. Zamawiający dopuszcza możliwość zmiany umowy w przypadku wystąpienia okoliczności niezależnych od stron, mających wpływ na termin lub sposób realizacji zamówienia.
7. Zamówienie realizowane jest w ramach projektu „Cyberbezpieczny Samorząd", współfinansowanego ze środków Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC).

ofertą należy złożyć podpisaną klauzulę informacyjną RODO stanowiącą załącznik nr 2 do niniejszego zapytania ofertowego.

4. Za termin złożenia oferty uznaje się datę i godzinę wpływu oferty do Zamawiającego.

XI. Osoby do kontaktu

W zakresie merytorycznym:
Dominik Śniecikowski-Robacki, e-mail: d.robacki@nowyduninow.info.pl
W zakresie składania ofert:
Rafał Winnicki, tel. 512 372 511, e-mail: r.winnicki@nowyduninow.info.pl

XII. Zakończenie postępowania

Zamawiający poinformuje Wykonawcę, którego oferta została uznana za najkorzystniejszą o terminie i miejscu zawarcia umowy. Otwarcie ofert nastąpi w dniu 19 czerwca 2026 r. w siedzibie Zamawiającego.

XIII. Załączniki

1. Formularz ofertowy
2. Klauzula informacyjna RODO
3. Wzór umowy
4. Wykaz osób skierowanych do realizacji zamówienia
5. Wzór Protokołu zdawczo-odbiorczego

WÓJT
Karol Gutkowicz