Cyberbezpieczny Samorząd

Strzelce, dnia 01 kwietnia 2025 r.

ZAPYTANIE OFERTOWE

na zamówienie publiczne o wartość nie przekraczającej 130 000 złotych (netto) prowadzone w oparciu o zasadę konkurencyjności zgodnie z zasadami określonymi w „Wytycznych w zakresie kwalifikowalności wydatków na lata 2021-2027" z dnia 18.11.2022 r.

Zapytanie realizowane jest w ramach projektu nr FERC.02.02-CS.01-001/23, pn. „Szkolenia SZBI i z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy Strzelce" - na potrzeby Konkursu Grantowego pn. „Cyberbezpieczny Samorząd", w ramach projektu „Cyberbezpieczny Samorząd w Gminie Strzelce" współfinansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021 - 2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

I. NAZWA I ADRES ZAMAWIAJĄCEGO:

Gmina Strzelce
ul. Leśna 1
99 – 307 Strzelce
NIP 775-24-06-139

II. TRYB UDZIELANIA ZAMÓWIENIA

1. Do niniejszego postępowania nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień Publicznych (t.j. Dz. U. z 2024 r. poz. 1320) zgodnie z art. 2 ust. 1 pkt 1 ustawy.
2. Wartość niniejszego zamówienia nie przekracza kwoty 50.000 złotych netto. Postępowanie prowadzone jest w formie zapytania ofertowego zgodnie z zasadami określonymi w Wytycznych dotyczących kwalifikowalności wydatków na lata 2021-2027.

III. PRZEDMIOT ZAMÓWIENIA:

- Szkolenia SZBI i z zakresu Cyberbezpieczenstwa dla pracowników i kadry zarządzającej,
- Szkolenia dla informatyka.

1. Przedmiotem zamówienia jest przeprowadzenie stacjonarnych szkoleń z zakresu cyberbezpieczeństwa dla pracowników, kadry zarządzającej, zakup platformy szkoleniowej dla pracowników, kadry zarządzającej oraz informatyka. Zamówienie obejmuje zakup dostępu do platformy szkoleniowej, na której pracownicy będą mogli na bieżąco szkolić się z zakresu cyberbezpieczeństwa.
2. Przedmiot zamówienia jest podzielony na 2 części.

Szkolenia (części 1 szkolenia dla pracowników i kadry zarządzającej, część 2 platforma szkoleniowa) muszą spełniać następujące wymagania:

1) Miejscem realizacji dla części 1 zamówienia jest siedziba Urzędu Gminy Strzelce przy ul. Leśnej 1, 99 – 307 Strzelce. Zamawiający może dopuścić zmianę jego formy w przypadku sytuacji nadzwyczajnych (pandemia, klęska żywiołowa, wprowadzenie stanu wyjątkowego, wojny, itp.), uniemożliwiających przeprowadzenie szkolenia stacjonarnego w Urzędzie. Miejscem realizacji dla części 2 – zakup szkolenia dziedzinowego dla pracowników, kadry zarządzającej oraz informatyka jest siedziba zamawiającego bądź możliwość szkolenia zdalnego na wniosek zamawiającego.
2) Szkolenia dla części 1 muszą odbywać się w godzinach pracy Urzędu.

3) Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji Zamawiającego.

4) Opracowane materiały będą musiały być dostarczone w formie elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF.

5) Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.

6) W ramach wynagrodzenia Wykonawca dostarczy Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowoprzyjętych.

7) Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat, potwierdzający ukończenie szkolenia i jego zakres.

8) Wykonawca powinien posiadać kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia. Osoby oddelegowane do przeprowadzenia szkolenia powinny spełniać wymagania doświadczenia zawodowego (praktyczne i/lub dydaktyczne) w zakresie wystąpień/ szkoleń/ prelekcji o tematyce podobnej w zakresie przedmiotu szkolenia. Na potwierdzenie doświadczenia Wykonawca dołączy do oferty Referencje potwierdzające realizację minimum 2 wystąpień/ szkoleń/ prelekcji o związanych z tematyką szkolenia przeprowadzonych w okresie ostatnich 3 lat od złożenia.

3. Część 1. Szkolenia dla pracowników, kadry zarządzającej Urzędu

W ramach realizacji części 1. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla pracowników, kadry zarządzającej w zakresie bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa. Celem szkolenia jest zwiększenie świadomości pracowników, kadry zarządzającej Urzędu w zakresie problematyki związanej z bezpieczeństwem informacji, rozwinięcie umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji.

Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje itp. co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.

Dla pracowników, kadry zarządzającej szkolenie musi obejmować co najmniej następującą tematykę:

- Omówienie zakresu niebezpieczeństw cybernetycznych, którym najczęściej poddane są instytucje administracji publicznej i samorządowej.
- Przegląd najczęstszych form ataków i ich konsekwencji dla instytucji administracji publicznej, w tym samorządowej oraz metod zmniejszania potencjalnego ryzyka w realizacji bieżących zadań - na przykładach z ostatnich 6 m-cy.

- Dostęp do obiektu instytucji administracji publicznej i samorządowej (ataki hackerskie typu "tailgating" i inne formy wejść i zagrożeń fizycznych).
- Podstawowe zasady higieny i bezpieczeństwa cyfrowego w jednostce administracji publicznej i samorządowej na przykładach: ataki wykorzystujące inżynierię społeczną, ataki złośliwym oprogramowaniem, próby wyłudzenia danych.
- Korzystanie z poczty elektronicznej - szyfrowanie danych, budowanie bezpiecznych haseł, zagrożenie przejęcia poczty firmowej i prywatnej, możliwe symptomy infekcji komputera.
- Uwierzytelnianie dwuskładnikowe - powody, metody, narzędzia.
- Metody zmniejszania potencjalnego ryzyka w realizacji bieżących zadań.
- Komunikacja kryzysowa – co należy zrobić w przypadku wystąpienia incydentu.
- Bezpieczeństwo danych instytucji administracji publicznej i samorządowej.
- Bezpieczna praca z przeglądarką:
    - Strony szyfrowane – jak rozpoznać strony szyfrowane i nieszyfrowane, co mówi nam oznaczenie https i kłódka, jak sprawdzić, czy strona jest bezpieczna, pułapki https, nowe oznaczenia szyfrowania.
    - Certyfikaty – co oznacza SSL, jak sprawdzić certyfikat strony, na co zwrócić uwagę.
- Prywatne działania w sieci i ekspozycja na zagrożenia cyfrowe instytucji publicznej i samorządowej:
    - Zagrożenia związane z używaniem poczty prywatnej do celów służbowych.
    - Potencjalne konsekwencje dla Urzędu wynikające z przejęcia prywatnego konta pracownika na portalu społecznościowym.
    - Zagrożenia wykorzystywania służbowych urządzeń mobilnych do celów prywatnych.
    - Bezpieczeństwo psychiczne w używaniu portali społecznościowych.
    - Wykorzystanie sztucznej inteligencji do ataków socjotechnicznych.
- Sprzęt firmowy, praca zdalna:
    - Na co warto zwrócić uwagę w kontekście bezpieczeństwa, pracując z domu lub w podróży.

Szkolenie powinno odbyć się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem co najmniej 4 przerw po 15 minut. Po szkoleniu przewidziano 30 minut na pytania i odpowiedzi uczestników.

Szkolenie dla pracowników i kadry zarządzającej powinno trwać co najmniej 4 dni.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić listę obecności z podpisami uczestników szkolenia.

Szkolenie musi być zakończone ankietą oceniającą szkolenie, jego przydatność, zakres przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

Dostęp do platformy szkoleniowej dla pracowników, kadry zarządzającej

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do zapewnienia pracownikom Zamawiającego dostępu do platformy szkoleniowej dla pracowników, kadry zarządzającej na okres 10 miesięcy. Na platformie szkoleniowej (e-learningowej) zamieszczone będą różnorodne materiały szkoleniowe z zakresu cyberbezpieczeństwa. Materiały szkoleniowe muszą być przez Wykonawcę na bieżąco uzupełniane i aktualizowane, zapewniającej prewencję w zakresie zagrożeń cyberbezpieczeństwa JST zwiększając świadomość oraz umożliwiając identyfikację nieprawidłowości lub luk systemów w obszarze działania jednostki. Aplikacja powinna być narzędziem ułatwiającym wdrożenie w JST środków zarządzania ryzykiem w cyberbezpieczeństwie oraz mechanizmów, procedur, procesów i środków zwiększających odporność na ataki z cyberprzestrzeni.

Udostępnienie platformy e-learningowej ma umożliwić pracownikom elastyczny dostęp do aktualnych informacji i standardowych praktyk w dogodnym dla nich czasie, co będzie sprzyjać skutecznej nauce, oraz poszerzenia wiedzy o inne tematy związane z cyberbezpieczeństwem.

Wykonawca zobowiąże się do udostępnienia platformy e-learningowej na niezmienionych warunkach technicznych, jakościowych i finansowych na co najmniej 3 miesiące po zakończeniu realizacji zamówienia.

Liczba użytkowników platformy – 21

Termin udostępnienia platformy (wraz z całością materiału szkoleniowego) – najpóźniej 30 dni po podpisaniu umowy.

Okres udostępnienia platformy –3 miesiące bez konieczności automatycznego odnawiania subskrypcji.

Platforma musi spełniać następujące wymagania:

Zawierać minimum 16 szkoleń, dostępnych w języku polskim.

Szkolenia dla pracowników i kadry zarządzającej muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
- Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu.
- Przegląd znanych typów ataków.
- Malware – złośliwe oprogramowanie.
- Phishing – podszycia pod inną tożsamość.
- Bezpieczne korzystanie z witryn internetowych.
- Testy socjotechniczne.
- Bezpieczeństwo fizyczne w ochronie informacji.
- Bezpieczna praca poza biurem i bezpieczeństwo urządzeń mobilnych.
- Bezpieczne hasła.
- Kryptografia w pracy urzędnika.
- Zarządzanie incydentem w urzędzie.
- Zarządzanie ryzykiem w bezpieczeństwie informacji.
- Ciągłość działania – wymagania (oparte na normie ISO 22301).
- Norma ISO 27001- omówienie, nowelizacja normy ISO 27002:2022
- SZBI – wymagania I procedury.

Film instruktażowy z udziałem lektora (5-30 minut), treści opisowe.

Konta indywidualne dla każdego użytkownika

Indywidualny certyfikat dla użytkownika po ukończeniu szkolenia

Testy sprawdzające wiedzę

Podstawowe funkcjonalności e-platformy:
- dostęp do szkoleń dla uczestników zgodnie z sugestiami Zamawiającego,
- szczegółowy zakres merytoryczny szkolenia;
- zadawania pytań merytorycznych
- wyjaśniane wątpliwości,
- zgłaszanie uwag technicznych,
- zmiana hasła przez uczestnika,
- wgląd do własnych aktywności,
- wgląd do aktywności grupy (dla wskazanego pracownika JST),
- możliwość uzyskania (wydrukowania) certyfikatu/świadectwa uczestnictwa w szkoleniu po spełnieniu ustalonych warunków.

Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

W ramach świadczonej usługi usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
- działać w przeglądarkach internetowych (Microsoft Edge, Mozilla Firefox i Google Chrome), bez konieczności instalowania dodatkowych komponentów po stronie klienta,
- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń (2 zmiany miesięcznie) lub liczby użytkowników (nie więcej niż 10% zmian w okresie trwania usługi),
- nowe lub zaktualizowane materiały szkoleniowe muszą być oznaczone jako „nowe",
  - umożliwiać zalogowanemu użytkownikowi pełen dostęp do wszystkich materiałów szkoleniowych i nieograniczony czas na zapoznanie się z materiałami szkoleniowymi przez cały czas dostępu do platformy,
  - po zakończeniu testu użytkownik musi mieć możliwość sprawdzenia swoich odpowiedzi i porównania ich z poprawnymi – poprawne odpowiedzi powinny być opatrzone komentarzem wyjaśniającym dlaczego właśnie ta odpowiedź jest poprawna.

4. Część 2.: Szkolenia dla informatyka

Szkolenie musi obejmować co najmniej następującą tematykę:
- kompleksowe szkolenie z narzędzia Extended Detection & Response (XDR) firmy ESET,
- szkolenie techniczne poświęcone urządzeniom do ochrony styku sieci firmowej z Internetem firmy STORMSHIELD.

5. Wymagania dodatkowe:

Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.
Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

6. Oznaczenie wg Wspólnego Słownika Zamówień (kod CPV):

80510000-2 Usługi szkolenia specjalistycznego
79632000-3 Szkolenie pracowników.

IV. Warunki udziału w postępowaniu.

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy **wykazali się niezbędną wiedzą i doświadczeniem w zakresie usług objętych niniejszym zapytaniem:**

1. na potwierdzenie spełniania warunku wiedzy i doświadczenia Wykonawca musi wykazać, że wykonał w okresie ostatnich trzech latach przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej **jedną usługę** szkoleń z zakresu cyberbezpieczeństwa dla pracowników i kadry zarządzającej **dla min. 30 osób** - zgodnie z **załącznikiem Nr 3** do niniejszego zapytania,

2. na potwierdzenie wykonania wyżej wymienionych usług Wykonawca zobligowany jest przedstawić dokumenty potwierdzające należyte wykonanie usług ujętych w wykazie (kserokopie dokumentów - referencje, protokoły odbioru, faktury), zadania nie potwierdzone dokumentami nie będą brane pod uwagę.

V. Wykluczenie z udziału w postępowaniu

1.Z postępowania o udzielenie zamówienia publicznego wyklucza się Wykonawców:

a) wobec, których zachodzą przesłanki wykluczenia określone w art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), dalej: rozporządzenie 833/2014, w brzmieniu nadanym rozporządzeniem Rady (UE) 2022/576 w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1), dalej: rozporządzenie 2022/576. Zgodnie z treścią art. 5k ust. 1 rozporządzenia 833/2014 w brzmieniu nadanym rozporządzeniem 2022/576 zakazuje się udzielania lub dalszego wykonywania wszelkich zamówień publicznych lub koncesji objętych zakresem dyrektyw w sprawie zamówień publicznych, a także zakresem art. 10 ust. 1, 3, ust. 6 lit. a)–e), ust. 8, 9 i 10, art. 11, 12, 13 i 14 dyrektywy 2014/23/UE, art. 7 i 8, art. 10 lit. b)–f) i lit. h)–j) dyrektywy 2014/24/UE, art. 18, art. 21 lit. b)–e) i lit. g)–i), art. 29 i 30 dyrektywy 2014/25/UE oraz art. 13 lit. a)–d), lit. f)–h) i lit. j) dyrektywy 2009/81/WE na rzecz lub z udziałem:

- obywateli rosyjskich lub osób fizycznych lub prawnych, podmiotów lub organów z siedzibą w Rosji;
- osób prawnych, podmiotów lub organów, do których prawa własności bezpośrednio lub pośrednio w ponad 50 % należą do podmiotu, o którym mowa w lit. a) niniejszego ustępu; lub
- osób fizycznych lub prawnych, podmiotów lub organów działających w imieniu lub pod kierunkiem podmiotu, o którym mowa w lit. a) lub b) niniejszego ustępu, w tym podwykonawców, dostawców lub podmiotów, na których zdolności polega się w rozumieniu dyrektyw w sprawie zamówień publicznych, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia.

b) zgodnie z treścią 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 (Dz. U. z 2024 roku, poz. 507) – t.j.:
   - wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   - wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124, 1285, 1723 i 1843) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   - wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

2. Zamawiający wykluczy z postępowania wykonawcę, który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

1. uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej,
2. posiadaniu co najmniej 10% udziałów lub akcji,
3. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
4. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

VI. KRYTERIA WYBORU NAJKORZYSTNIEJSZEJ OFERTY I ICH WAGI PROCENTOWE:

- Cena najniższa **100 %**

VII. OPIS SPOSOBU OBLICZENIA CENY OFERTY.

1. Cenę należy wyliczyć jako sumę poszczególnych pozycji składających się na przedmiot zamówienia.
2. Wykonawca musi uwzględnić w cenie oferty wszystkie koszty niezbędne do prawidłowego i pełnego wykonania zamówienia.
3. Cenę oferty podać w PLN z dokładnością do dwóch miejsc po przecinku.

Opis przyznawania punktacji - sposobu przyznawania punktacji za spełnienie danego kryterium oceny Oferty:

Cena przedmiotu zamówienia – obejmuje cenę wykonania usługi. Oferta z najniższą ceną otrzyma maksymalną ilość punktów = **100 pkt.**, oferty następne będą oceniane na zasadzie proporcji w stosunku do oferty najtańszej wg wzoru:

$$C = [C_{min} / C_{bad}] \times 100$$

gdzie:

- C - liczba punktów za cenę ofertową
- C_{min} - najniższa cena ofertowa spośród ofert badanych
- C_{bad} - cena oferty badanej

Opis: Uzyskana z wyliczenia ilość punktów zostanie ostatecznie ustalona z dokładnością do drugiego miejsca po przecinku z zachowaniem zasady zaokrągleń matematycznych.

Oferta Wykonawcy, która otrzyma najwyższą liczbę punktów zostanie uznana za najkorzystniejszą. Jeżeli nie można dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

W sytuacji gdy cena najkorzystniejszej oferty będzie znacząco przewyższała środki zabezpieczone przez Zamawiającego w budżecie, Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych negocjacji z Wykonawcą który złoży najkorzystniejszą ofertę.

VIII. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT:

1. Podpisaną ofertę wraz z wymaganymi załącznikami należy złożyć **do dnia 9 kwietnia 2025 roku do godz. 09:00** w formie pisemnej lub w postaci skanu w jeden z następujących sposobów:
   - w sekretariacie gminy adres: Urząd Gminy Strzelce, ul. Leśna 1, 99-307 Strzelce,
   - na maila Zamawiającego na adres: sekretariat@gminastrzelce.eu .
2. Oferty złożone po terminie podlegają odrzuceniu i nie będą rozpatrywane.
3. Zamawiający nie przewiduje publicznej sesji otwarcia ofert.
4. W toku badania i oceny ofert Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert.
5. Informacja o możliwości składania ofert częściowych
   Zamawiający nie przewiduje możliwości składania ofert częściowych.
6. Opis sposobu przedstawiania ofert wariantowych oraz minimalne warunki, jakim muszą odpowiadać oferty wariantowe wraz z wybranymi kryteriami oceny, jeżeli zamawiający wymaga lub dopuszcza ich składanie: **Zamawiający nie dopuszcza złożenia oferty**

wariantowej.

7. Zamawiający nie przewiduje zamówień „uzupełniających".

IX. WARUNKI ZAWARCIA UMOWY ORAZ WARUNKI JEJ ZMINY:

1. Umowa w sprawie realizacji zamówienia zawarta zostanie z uwzględnieniem postanowień wynikających z treści niniejszego zapytania wraz z załącznikami. Wzór umowy stanowi **załącznik nr 4** do zapytania ofertowego.
2. Zamawiający podpisze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę według przyjętego kryterium.
3. Zamawiający zastrzega sobie prawo zmiany treści umowy po jej podpisaniu. Zmiany te mogą dotyczyć:
   a) wystąpienia uzasadnionych zmian w zakresie i sposobie wykonania przedmiotu zamówienia;
   b) wystąpienia obiektywnych przyczyn niezależnych od Zamawiającego i Wykonawcy;
   c) wystąpienia okoliczności będących wynikiem działania siły wyższej;
   d) zmiany istotnych regulacji prawnych;
   e) zmiany w zawartej umowie o dofinansowanie grantu;
   f) gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy.
4. Jeżeli wybrany Wykonawca uchyla się od zawarcia umowy, najkorzystniejsza oferta może zostać wybrana spośród ofert pozostałych, bez przeprowadzenia ich ponownej oceny.

X. INFORMACJE DODATKOWE:

1. **Zamawiający może w każdym czasie, przed udzieleniem niniejszego zamówienia publicznego, unieważnić przedmiotowe postępowanie bez podania przyczyny.**
2. Zamawiający zastrzega sobie prawo prowadzenia negocjacji z wybranym Wykonawcą.
3. Niniejsze Zapytanie Ofertowe nie stanowi przetargu w rozumieniu przepisów Kodeksu Cywilnego ani Ustawy Prawo zamówień publicznych. Zamawiający nie jest zobowiązany do wyboru jakiejkolwiek oferty, a złożenie oferty nie stanowi podstawy do wystąpienia z jakimkolwiek roszczeniem wobec Zamawiającego ze strony podmiotu, który złożył ofertę.
4. Zamawiający nie przewiduje składania ofert częściowych.
5. Osobą uprawnioną do kontaktowania się z Wykonawcami i udzielania wyjaśnień dotyczących postępowania jest Andrzej Wojtczak, tel. 502 585 724, e-mail: a.wojtczak@pro.onet.pl.
6. W toku badania ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty, treści oświadczeń, dokumentów, pełnomocnictw i ich uzupełnienia.
7. Zamawiający odrzuci ofertę Wykonawcy, który nie udzieli wyjaśnień, o których mowa powyżej.
8. Zamawiający wyjaśni i poprawi w formularzu ofertowym:
   oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, inne omyłki polegające na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Poprawienie przez Zamawiającego oczywistych omyłek pisarskich oraz rachunkowych i konsekwencji rachunkowych dokonanych poprawek nie wymaga uzyskania zgody wykonawcy. Wykonawca może nie wyrazić zgody na poprawienie przez zamawiającego innych omyłek polegających na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Brak zgody Wykonawca musi wnieść na piśmie w wyznaczonym przez Zamawiającego terminie.

9. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, na każdym etapie prowadzonego postępowania. Z tytułu unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.
10. W przypadku gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie przez Zamawiającego umowy z kolejnym Wykonawcą, który w postępowaniu uzyskał kolejną najwyższą liczbę punktów.

XI. KLAUZULA INFORMACYJNA RODO

Na podstawie art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. z 2016 r. Nr 119, str. 1) – (zwanym w dalszej części „RODO") informujemy, że:

1. Administratorem Państwa danych osobowych przetwarzanych w Urzędzie Gminy Strzelce jest Wójt Gminy Strzelce, 99-307 Strzelce, ul. Leśna 1;
2. Inspektorem ochrony danych osobowych u administratora jest Aneta Pacholska, e-mail: a.pacholska01@gmail.com, tel. 665 973 770;.
3. Państwa dane osobowe przetwarzane będą:

a) w celu związanym z realizacją postępowania o udzielenie zamówienia publicznego prowadzonego w trybie zapytania ofertowego w szczególności rejestracji składanych ofert, rozpatrywania złożonych ofert, wyboru dostawcy/wykonawcy – na podstawie art. 6 ust. 1 lit. c RODO w związku z ustawą z dnia 27 sierpnia 2009 r. o finansach publicznych oraz ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych;
b) w celu przygotowania i podpisania umowy na wykonanie przedmiotu zamówienia – jeżeli taka zostanie z Państwem zawarta - na podstawie art. 6 ust. 1 lit. b RODO
c) w celu wypełnienia obowiązków prawnych ciążących na Administratorze wynikających z obowiązujących przepisów prawa, w szczególności związanych z archiwizacją dokumentacji– zgodnie art. 6 ust. 1 lit. c RODO;

4. Odbiorcami Państwa danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o ustawę o dostępie do informacji publicznej z dnia 26 września 2001 r. oraz inne podmioty upoważnione na podstawie przepisów prawa oraz instytucje na mocy wiążących umów (np. w celu rozliczenia środków publicznych). Odbiorcą może być również dostawca usług hostingowych (dostawca usługi poczty e-mail) oraz operator pocztowy.
5. Państwa dane osobowe będą przez okres niezbędny do realizacji celów przetwarzania, lecz nie krócej niż okres wskazany w przepisach o archiwizacji tj. przez okres 5 pełnych lat od dnia zakończenia postępowania o udzielenie ww. zamówienia.
6. W odniesieniu do Państwa danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
7. Posiadają Państwo:
   - na podstawie art. 15 RODO prawo żądania dostępu do danych osobowych Państwa dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Państwa danych osobowych;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają Państwo, że przetwarzanie danych osobowych Państwa dotyczących narusza przepisy RODO;

8. Nie przysługuje Państwu:
   - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Państwa danych osobowych jest art. 6 ust. 1 lit. c RODO.
9. W oparciu o udostępnione dane osobowe Administrator nie będzie podejmował wobec Państwa zautomatyzowanych decyzji, w tym decyzji będących wynikiem profilowania.

XI. **<u>Załączniki (wzory dokumentów) które mają być złożone w ramach oferty:</u>**
   - Załącznik nr 1 - Formularz oferty,
   - Załącznik nr 2 - Oświadczenie o braku podstaw do wykluczenia,
   - Załącznik nr 3 –Wykaz usług
   - Załącznik nr 4 – Wzór umowy

z up. WÓJTA
Wioleta Maćczak
SEKRETARZ GMINY