

Korytnica, dnia 09.06.2026 roku

ZAPYTANIE OFERTOWE

Przedmiot zamówienia obejmuje:

Przeprowadzenie szkoleń z zakresu podstaw cyberbezpieczeństwa (budujących świadomość cyberzagrożeń i sposobów ochrony) dla kadry kierowniczej i kadry pracowniczej jednostek:

1. Urząd Gminy Korytnica,
2. Gminny Ośrodek Pomocy Społecznej w Korytnicy
3. Gminny Zespół Ekonomiczno-Administracyjny Szkół w Korytnicy
4. Zespół Szkolno-Przedszkolny w Korytnicy
5. Szkoła Podstawowa w Pniewniku
6. Szkoła Podstawowa w Sewerynowie
7. Szkoła Podstawowa w Górkach-Grubakach

I. ZAMAWIAJĄCY

Gmina Korytnica
ul. Adama Małkowskiego 20
07-120 Korytnica
NIP: 824 17 27 162

II. POSTANOWIENIA OGÓLNE

Do udzielenia przedmiotowego zamówienia nie stosuje się przepisów Ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych.

Procedura postępowania będzie prowadzona zgodnie z Wytycznymi dotyczącymi kwalifikowalności wydatków na lata 2021-2027 i dokumentami wydanymi na podstawie art. 6 ust. 2 ustawy wdrożeniowej.

Projekt współfinansowany jest z Programu „Cyberbezpieczny samorząd”, w ramach środków z FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1 Przedmiot zamówienia, podmioty objęte usługą oraz terminy realizacji:

- a) Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu podstaw cyberbezpieczeństwa (budujących świadomość cyberzagrożeń i sposobów ochrony) dla **kadry kierowniczej** siedmiu wyżej wymienionych jednostek

Wymagania co do organizacji szkoleń:

- szkolenia przeprowadzone online lub na platformie szkoleniowej; niezależnie od formy przeprowadzenia, **dostęp do nagrania ze szkolenia będzie dostępny online przez 30 dni za pomocą łatwo dostępnego środka dla Zamawiającego np. platforma internetowa lub chmura, bez konieczności rejestracji konta na adres e-mail, dostęp poprzez link.**
- czas trwania szkolenia: max. 3 godziny;
- ilość Uczestników szkolenia: 13 osób,
- terminy realizacji: od. 18.06.2026 r do 30.07.2026 r.
- szkolenie zakończone wystawieniem certyfikatów dla każdego Uczestnika.

- b) Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu podstaw cyberbezpieczeństwa (budujących świadomość cyberzagrożeń i sposobów ochrony) dla **kadry pracowniczej** siedmiu wyżej wymienionych jednostek

Wymagania co do organizacji szkoleń:

- szkolenia przeprowadzone online lub na platformie szkoleniowej; niezależnie od formy przeprowadzenia, **dostęp do nagrania ze szkolenia będzie dostępny online przez 30 dni za pomocą łatwo dostępnego środka dla Zamawiającego np. platforma internetowa lub chmura, bez konieczności rejestracji konta na adres e-mail, dostęp poprzez link.**
- czas trwania szkolenia: max. 3 godziny dla każdej grupy;
- ilość Uczestników szkoleń: 103 osób, podzielonych **na 2 grupy**
- terminy realizacji: od 18.06.2026 r do 30.07.2026 r.
- szkolenie zakończone wystawieniem certyfikatów dla każdego Uczestnika.

2. Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy zakres szkoleń najpóźniej 2 dni kalendarzowych przed uzgodnionym terminem realizacji szkolenia. Minimalny zakres szkolenia dla obydwu grup musi zawierać poniższe oraz być dostosowany do grupy docelowej (kadra kierownicza/kadra pracownicza):

Tematyka szkolenia zawierać będzie omówienie poprawnych zasad związanych z cyberbezpieczeństwem. Ponadto muszą zostać omówione zagrożenia w sieci takie jak phishing, ransomware oraz malware, które powodują poważne zagrożenia dla bezpieczeństwa informacji. Na szkoleniu poruszone muszą zostać również sposoby przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami, co w stopniu wyższym podniesie wiedzę uczestników z zakresu cyberbezpieczeństwa.

- Wprowadzenie do cyberprzestępczości: Podstawy cyberbezpieczeństwa.
- Zorganizowane grupy cyberprzestępcze: Jak działają i dlaczego są groźne.
- Czy cyberprzestępcy naprawdę nam zagrażają?
- Czy jestem atrakcyjnym klientem dla cyberprzestępcy?
- Korzyści dla cyberprzestępców: Co zyskują atakując Twoje dane?
- Rodzaje ataków na pracowników biurowych.
- Straty dla JST: Skutki udanego cyberataku.
- Sieci Botnet: Jak cyberprzestępcy przejmują komputery.
- Skuteczne metody ochrony przed cyberatakami.
- AI w rękach cyberprzestępców: Nowe zagrożenia z wykorzystaniem sztucznej inteligencji.
- Spam jako niegroźny sposób na groźne ataki.
- Czy cyberprzestępcy są zawsze anonimowi?
- Phishing jako metoda okradania naszych kont bankowych.
- Ataki DoS/DDoS: Zagrożenia dla instytucji.
- Ataki 0-day: Czy istnieje sposób obrony przed nimi?
- Opłaconą fakturę jako sposób przemyślenia wirusa do naszego systemu.
- Bezpieczeństwo haseł: Jak cyberprzestępcy zdobywają Twoje hasła?
- Skanowanie kart płatniczych: Gdzie i kiedy ktoś może zeskanować Twoją kartę?
- Ataki socjotechniczne, czyli niewinne wyłudzenie danych.
- Kradzież tożsamości: Co? Jak? Kiedy? Gdzie?
- Bezpieczne przekazywanie haseł współpracownikom.
- Fizyczne bezpieczeństwo: Jak zabezpieczyć miejsce pracy.
- Znalezione pendrive, jako pozwolenie na atak cyberprzestępcy.
- Zwiększenie odporności na cyberataki: Proste i skuteczne metody.
- Sprzęt prywatny vs. firmowy: Jak zarządzać bezpieczeństwem urządzeń.
- Panel Q&A

3. Zrealizowanie szkoleń musi zostać potwierdzone protokołem odbioru, podpisanym przez Wykonawcę i Zamawiającego.
4. Podpisanie protokołu odbioru upoważnia Wykonawcę do wystawienia faktury.
5. Brak rozpoczęcia działań w terminie 30 dni kalendarzowych od terminu złożenia oficjalnego zamówienia, upoważnia Zamawiającego do odstąpienia od zamówienia.

IV. WARUNKI UDZIAŁU W POSTĘPOWANIU

W postępowaniu mogą wziąć udział wykonawcy, którzy:

1. są zdolni do wykonania przedmiotu zamówienia i spełniają warunki w zakresie:
 - a) posiadania kompetencji/uprawnień do prowadzenia działalności zawodowej, o ile wynika to z odrębnych przepisów – złożą w tym zakresie oświadczenie na formularzu ofertowym;
 - b) sytuacji finansowej umożliwiającej realizację przedmiotu zamówienia – złożą w tym zakresie oświadczenie na formularzu ofertowym;
 - c) posiadania potencjału technicznego i osobowego niezbędnego do wykonania przedmiotu zamówienia:
 - Wykonawcy biorący udział w zapytaniu muszą wykazać, że osoba odpowiedzialna za przeprowadzenie szkolenia posiada stosowną wiedzę i m.in. 2 letnie doświadczenie oraz co najmniej 1 certyfikat świadczący o posiadanej wiedzy tj. certyfikat audytora wiodącego ISO 27001 lub pokrewne.
 - d) posiadania wiedzy i doświadczenia w wykonywaniu przedmiotu zamówienia - złożą w tym zakresie oświadczenie na formularzu ofertowym;
 - e) złożą formularz ofertowy według wzoru stanowiącego załącznik nr 1 do zapytania ofertowego wraz z oświadczeniami.

V. OPIS SPOSOBU PRZYGOTOWANIA OFERTY, WYMAGANE DOKUMENTY I UPRAWNIENIA

Wykonawca składa ofertę na **formularzu ofertowym wraz z oświadczeniami** załączonymi do niniejszego zapytania. Zamawiający nie dopuszcza możliwość składania ofert na każdą część oddzielnie. Złożona oferta obejmuje koszt łączny wszystkich części wyrażony w kwocie netto i brutto.

VI. MIEJSCE, SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Zamawiający wymaga, aby formularz ofertowy został **podpisany cyfrowo**. Dopuszcza się podpisanie oferty kwalifikowanym podpisem elektronicznym, podpisem zaufanym (ePUAP) lub podpisem osobistym
2. Oferta powinna zostać dostarczona w terminie do dnia 17.06 2026 r. do godz. 09:00 pocztą elektroniczną na adres ug@korytnica.pl
2. O zachowaniu terminu decyduje data wpływu oferty do Zamawiającego. Oferty, które wpłyną po wskazanym terminie nie będą rozpatrywane.
3. O wyniku postępowania zamawiający poinformuje wykonawców drogą mailową.
4. Oferent może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
5. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.

VII. OCENA OFERT

Zamawiający dokona oceny ważnych ofert w oparciu o kryterium ceny.
Cena brutto: 100% (najniższa cena = 100 pkt, proporcja liniowa dla pozostałych).

VIII. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY

O wyborze najkorzystniejszej oferty Zamawiający zawiadomi wykonawców w formie pisemnej/telefonicznej lub drogą mailową.

Zamawiający zastrzega sobie możliwość unieważnienia postępowania bez podania przyczyny.

IX. ZAŁĄCZNIKI

1. Formularz ofertowy;
2. Oświadczenie o braku przesłanek;
3. Oświadczenie o braku podstaw wykluczenia;
4. Oświadczenie o braku powiązań osobowych i kapitałowych;
5. Projekt umowy
6. Projekt umowy PDDO

