



## Zapytanie ofertowe nr 271.21B.2024

na

### przeprowadzenie cyklu szkoleń dla pracowników Zamawiającego w zakresie cyberbezpieczeństwa

#### I. ZAMAWIAJĄCY NAZWA I ADRES

Zamawiającym jest:

Gmina Perzów reprezentowana przez :

Wójta Gminy Perzów

Perzów 78

63-642 Perzów

tel.: 062 786 1850

faks: 062 786 1509

e-mail: [gmina@perzow.pl](mailto:gmina@perzow.pl)

strona internetowa: [www.perzow.pl](http://www.perzow.pl), [www.perzow.nowoczesnagmina.pl](http://www.perzow.nowoczesnagmina.pl)

#### II OZNACZENIE POSTĘPOWANIA

Postępowanie oznaczone jest jako ROŚGPK.271.21B.2024

Wszelka korespondencja oraz dokumentacja w tej sprawie będzie powoływać się na wyżej wymienione oznaczenie.

#### III PRZEDMIOT ZAMÓWIENIA ORAZ WARUNKI ZAMÓWIENIA

1. Przedmiotem zamówienia jest przeprowadzenie szkolenia dla pracowników Zamawiającego w zakresie cyberbezpieczeństwa, dotyczącego praktycznego stosowania mechanizmów bezpieczeństwa korespondencji i zabezpieczania danych, w ramach projektu konkursu grantowego pn. „Cyberbezpieczny Samorząd” realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Priorytet II: Zaawansowane usługi cyfrowe (dalej: konkurs „Cyberbezpieczny Samorząd”).
2. W szkoleniu będzie brało udział 25 osób podzielonych na trzy grupy, z których dla każdej grupy przeznaczony będzie jeden dzień szkolenia w pełnym zakresie informacji. Szkolenia odbędą się w siedzibie Zamawiającego w godzinach 7-15.
3. Szkolenie powinno składać się z części teoretycznej i praktycznej.
4. Szczegółowy zakres szkolenia teoretycznego powinien obejmować co najmniej następujące zagadnienia:
  - 4.1. Wprowadzenie do bezpieczeństwa cyfrowego w organizacji





## Cyberbezpieczny Samorząd

- 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.
- 4.2. Cyfrowe bezpieczeństwo fizyczne. Podstawowe zasady bezpieczeństwa fizycznego w kontekście możliwych ataków cyfrowych:
- Dostęp do obiektu instytucji administracji publicznej i samorządowej (ataki hackerskie typu "tailgating" i inne formy wejść i zagrożeń fizycznych).
  - Zapewnienie bezpieczeństwa fizycznego dla dokumentów fizycznie umieszczonych w budynku instytucji.
  - Dostęp fizyczny do sprzętu i oprogramowania IT w firmie, w tym zewnętrzne nośniki pamięci cyfrowej.
- 4.3. Cyberbezpieczeństwo:
- 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.
- 4.4. Bezpieczeństwo danych instytucji administracji publicznej i samorządowej – czynnik ludzki:
- Rozmowy o pracy w miejscach publicznych – zasady bezpiecznych rozmów, czego unikać, jak ograniczyć ryzyko.
  - Udostępnianie zewnętrzne – zasady kwalifikacji, przesyłanie danych e-mailem, przenoszenie na pendriv-ie, korzystanie z nośników reklamowych, wykorzystanie folderów dzielonych i tymczasowych, szyfrowanie.
  - Makra – wykorzystanie do ataków, kiedy włączać makra, jak unikać zagrożeń.
  - Usuwanie danych – jak zadbać o dane, jak przechowywać dane, miejsca przechowywania danych.
  - RODO – podstawowe wymagania, jak działać zgodnie z RODO, na co zwracać uwagę w codziennej pracy.
- 4.5. 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.
- 4.6. 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.
- 4.7. Sprzęt firmowy, praca zdalna:



## Cyberbezpieczny Samorząd

- Na co warto zwrócić uwagę w kontekście bezpieczeństwa, pracując z domu lub w podróży.
5. Oprócz szkolenia teoretycznego Wykonawca powinien zrealizować ćwiczenia praktyczne obejmujące tematykę szkolenia (np. w formie Quiz/gry lub ćwiczenia).
  6. Wykonawca zobowiązany jest przeprowadzić testy sprawdzające wiedzę – na wstępie szkolenia i na jego zakończeniu. Po zakończeniu szkolenia, zostanie udostępniona ankieta ewaluacyjna szkolenia, a wynik ankiety w formie raportu zostanie przekazany Zamawiającemu.
  7. Dokumentowanie prowadzonych zajęć i działań nastąpi poprzez prowadzenie list obecności, na drukach oznaczonych logotypami, przygotowanych przez Zamawiającego. Listy obecności zostaną przekazane Zamawiającemu niezwłocznie po przeprowadzeniu szkolenia.
  8. Wykonawca jest zobowiązany w terminie do 7 dni kalendarzowych po zakończeniu realizacji Przedmiotu zamówienia dostarczyć certyfikaty ukończenia szkolenia, zgodnie z listą obecności.
  9. Zamawiający wskazuje jako miejsce przeprowadzenia szkolenia siedzibę Zamawiającego lub inną lokalizację wskazaną przez Zamawiającego w odległości do 10 km od siedziby Zamawiającego. Rezerwacja miejsca prowadzenia zajęć jest po stronie i na koszt Zamawiającego.
  10. Ekran odpowiedniej wielkości lub rzutnik Wykonawca zapewni we własnym zakresie. Zamawiający zapewni również dostęp do energii elektrycznej (gniazdka).
  11. W szkoleniu będzie brało udział 25 osób podzielonych na trzy grupy, z których dla każdej grupy przeznaczony będzie jeden dzień szkolenia w pełnym zakresie informacji. Szkolenia odbędą się w siedzibie Zamawiającego w godzinach 7-15.
  12. Wykonawca zobowiązuje się w terminie 7 dni od dnia podpisania umowy dostarczyć Zamawiającemu:
    - 1) proponowane terminy szkolenia;
    - 2) szczegółowy zakres merytoryczny szkolenia;
    - 3) dzienny harmonogram szkolenia.Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia. Szkolenia będą przeprowadzone po ostatecznej akceptacji dokumentacji przez Zamawiającego.
  13. W ramach organizacji szkolenia Wykonawca zapewni:
    - 1) materiały szkoleniowe, obejmujące szczegółowy zakres merytoryczny szkolenia i harmonogram dzienny szkolenia (materiały zostaną przekazane każdemu uczestnikowi szkolenia w wersji elektronicznej – nieodpłatnie, na własność);
    - 2) oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom (zgodnie z zasadami określony w konkursie „Cyberbezpieczny Samorząd”);
    - 3) wydanie Zamawiającemu szkolenia zaświadczeń/certyfikatu o ukończeniu szkolenia dla każdego uczestnika;
    - 4) kadre trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia;





## Cyberbezpieczny Samorząd

### V TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca zobowiązany jest zrealizować usługę w terminie **do 30.11.2024 r.**

### VI WARUNKI UDZIAŁU W POSTĘPOWANIU

O udzielenie zamówienia ubiegać mogą się Wykonawcy, którzy posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do należytego i terminowego wykonania zamówienia. Zamawiający uzna warunek za spełniony, jeżeli:

1. Posiada doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń – w tym celu Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – przeprowadził min. jedno szkolenie cyberbezpieczeństwa;
2. Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej 1 osobą, która przeprowadziła co najmniej 1 szkolenie z obszaru cyberbezpieczeństwa

### VII KRYTERIA OCENY OFERT

1. Kryteria, którymi Zamawiający będzie kierował się przy wyborze oferty wraz z podaniem znaczenia (wag) tych kryteriów:
  1. Cena – 60 % (60 pkt)
  2. doświadczenie – 40 % (40 pkt)
2. Ocena ofert:
  - 1) Opis kryterium Cena (C):

Ocena w niniejszym kryterium zostanie dokonana według następującego wzoru:

$$C = \frac{\text{Najniższa cena brutto przedstawiona w ofertach na realizację zamówienia}}{\text{Cena brutto na realizację zamówienia badanej oferty}} \times 60$$

- 2) Opis kryterium doświadczenie szkolenie z obszaru cyberbezpieczeństwa:
  - a)Przeprowadzone 1 szkolenie: 0 pkt
  - b)Przeprowadzone 2 szkolenia:10 pkt
  - c)Przeprowadzone 3 szkolenia:20 pkt
  - d)Przeprowadzone 4 szkolenia:30 pkt
  - e)Przeprowadzone 5 i więcej szkoleń:40 pkt

Przeprowadzone szkolenia winny potwierdzone być referencjami.

3. Łączna ocena ofert zostanie obliczona według wzoru: Suma = Cena + Doświadczenie.
4. Łączna maksymalna liczba punktów, jaką można przyznać ofercie za wszystkie kryteria wynosi 100 pkt. Przyjmuje się, że 1 pkt równa się 1%. Punktacja przyznana ofertom w poszczególnych kryteriach będzie liczona z dokładnością do dwóch miejsc po przecinku.





## Cyberbezpieczny Samorząd

### VIII SPOSÓB PRZYGOTOWANIA OFERTY

1. Każdy Wykonawca może złożyć tylko jedną ofertę w niniejszym postępowaniu.
2. Ofertę stanowi:
  - a) Wypełniony formularz oferty sporządzony zgodnie ze wzorem stanowiącym załącznik nr 1 do Zapytania ofertowego;
  - b) Pełnomocnictwo dla osoby/osób podpisującej ofertę i oświadczenia (jeśli uprawnienie tych osób nie wynika z innych dokumentów dołączonych do oferty).
3. Oferta powinna:
  - a) być złożona w formie pisemnej, zgodnie z wymaganiami opisanymi w niniejszym zapytaniu.
  - b) być sporządzona w języku polskim, w sposób czytelny na komputerze, maszynie lub pismem odręcznym.
  - c) ponumerowana,
  - d) posiadać wszystkie dane Wykonawcy (tj. adres lub siedzibę oferenta, numer telefonu, numer NIP,) i winna być podpisana przez osobę reprezentującą Wykonawcę
  - e) posiadać datę sporządzenia,
  - f) być wypełniona w formularzu ofertowym w zakresie wszelkich informacji
4. Termin związana ofertą wynosi 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
5. Koszty związane z przygotowaniem oferty ponosi składający ofertę. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
6. Oferta Wykonawcy winna spełniać wszystkie wymagania określone w niniejszym zapytaniu, a także zawierać wszystkie żądane dokumenty i załączniki.
7. Zaleca się aby oferta została sporządzona na formularzu stanowiącym Załącznik do niniejszego zapytania.

### IX MIEJSCE I TERMIN ZŁOŻENIA OFERTY

1. Oferta powinna być przesłana za pośrednictwem:
  - poczty tradycyjnej na adres Perzów 78, 63-642 Perzów,
  - poczty e-mail na adres [przetargi@perzow.pl](mailto:przetargi@perzow.pl),
  - kuriera lub też dostarczona osobiście na adres: Perzów 78, 63-642 Perzów,
  - w wersji elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym za pośrednictwem e-puap do dnia 12.09.2024 r. do godz. 10:00.
2. Ocena ofert zostanie dokonana niezwłocznie po terminie otwarcia ofert.
3. Oferty złożone po terminie nie będą rozpatrywane
4. W toku badania i oceny ofert Zamawiający może żądać od oferentów wyjaśnień dotyczących treści złożonych ofert.
5. Oferta do terminu składania ofert stanowi własność Wykonawcy.
6. Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed terminem składania ofert.
7. Zamawiający zastrzega sobie prawo negocjacji warunków objętych odpowiedzią na zapytanie ofertowe poprzez zaproszenie do bezpośredniej rozmowy w siedzibie Zamawiającego.
8. Złożenie ofert nie jest wiążące dla Zamawiającego.
9. Wykonawcy, których oferty nie zostaną wybrane nie mogą zgłaszać żadnych roszczeń względem Zamawiającego z tytułu otrzymania niniejszego zapytania ofertowego oraz przygotowania i złożenia oferty na to zapytanie.
10. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyny.





## Cyberbezpieczny Samorząd

### X OSOBY UPOWAŻNIONE DO KONTAKTÓW Z WYKONAWCAMI

1. Osobą uprawnioną przez Zamawiającego do kontaktu jest:  
Agnieszka Smolarek – w sprawach procedury udzielenia zamówienia, adres email : [agnieszka.smolarek@perzow.pl](mailto:agnieszka.smolarek@perzow.pl) ; tel. 62 78 61 853;  
Natalia Świerblewska – w sprawach przedmiotu zamówienia, adres email: [natalia.swierblewska@perzow.pl](mailto:natalia.swierblewska@perzow.pl) ; tel. 62 78 61 067;
2. Każdy Wykonawca ponosi ryzyko związane z ewentualną wadliwością informacji uzyskanych od osób trzecich, niewymienionych w pkt. 1.
3. Wszystkie informacje dotyczące postępowania o zamówienie publiczne będą przekazywane Wykonawcom przez Zamawiającego drogą elektroniczną,  
Taki sam sposób porozumiewania się z Zamawiającym obowiązuje Wykonawcę.
5. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści zapytania. Zamawiający może udzielić wyjaśnień jeżeli uzna, że zapytanie będzie miało wpływ na treść składanej oferty.

### XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca zostanie związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

### XII WYBÓR OFERTY

1. Po upływie terminu wyznaczonego do składania ofert Zamawiający dokona ich analizy i oceny zgodnie z zasadami określonymi w niniejszym zapytaniu.
2. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert lub uzupełnienia dokumentów wymaganych w zapytaniu.
3. W przypadku, gdy zaoferowana cena budzi wątpliwości Zamawiającego, co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w zapytaniu ofertowym, Zamawiający zwraca się o udzielenie wyjaśnień dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na Wykonawcy.
4. Jeżeli nie można wybrać oferty z uwagi na fakt, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów, Zamawiający zaprasza Wykonawców, którzy złożyli oferty, do złożenia ofert dodatkowych w wyznaczonym przez siebie terminie. Niedopuszczalne jest złożenie cen wyższych niż w złożonych ofertach.
5. W przypadku, gdy cena złożonych ofert przewyższa kwotę, którą Zamawiający może przeznaczyć na sfinansowanie zamówienia prowadzący postępowanie może zaprosić Wykonawców, którzy złożyli oferty, do złożenia ofert dodatkowych w wyznaczonym przez siebie terminie. Niedopuszczalne jest złożenie cen wyższych niż w złożonych ofertach.
6. O wyborze oferty/unieważnieniu postępowania Zamawiający powiadomi wszystkich Wykonawców składających oferty.
7. Zamawiający w każdej chwili może unieważnić postępowanie na każdym jego etapie, bez podania przyczyny.

### XIII. INFORMACJA O PODWYKONAWSTWIE

1. W związku ze specyfiką zamówienia i udostępniania Wykonawcy, zobowiązanego do podpisania klauzuli poufności, w szerokim zakresie różnorodnych danych, niezbędnych do wykonania przedmiotu zamówienia Zamawiający nie dopuszcza Podwykonawców przy realizacji zamówienia.

### XIV ZAŁĄCZNIKI

- 1) Formularz ofertowy;
- 2) Wzór umowy.

WÓJT  
mgr Danuta Froń



## Cyberbezpieczny Samorząd

### **Klauzula RODO**

Ochrona danych osobowych Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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. Urz. UE L 119

z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- Administratorem Pani/Pana danych osobowych jest Wójt Gminy Perzów, Gmina Perzów, 63-642 Perzów 78;
- Administrator wyznaczył Inspektora Ochrony Danych Osobowych w Urzędzie Gminy Perzów. Dane kontaktowe: Monika Idźczak, iod@perzow.pl;

Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem.

- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania

w oparciu o art. 18 ustawy z dnia 11 września 2019 r. –Prawo zamówień publicznych, dalej „ustawa Pzp”;

- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

▪ obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO; w posiada Pani/Pan: — na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących; — na podstawie art. 16 RODO prawo do sprostowania Pani/Pana 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 uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO; nie przysługuje Pani/Panu: — 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 Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.



