



Cyberbezpieczny Samorząd

ZAPYTANIE OFERTOWE

prowadzone zgodnie z zasadą konkurencyjności o wartości poniżej kwoty 130.000 zł na realizację zadania pn.:

**„Usługi wsparcia w realizacji projektu w tym wprowadzenie lub aktualizacja dokumentacji SZBI,
dostarczenie narzędzi do analizy ryzyka oraz przeprowadzenie szkoleń”
w ramach projektu grantowego pn. „Cyberbezpieczny Powiat Nidzicki (skrót CPN)”
dofinansowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027**

1. Zamawiający:

Powiat Nidzicki
ul. Traugutta 23, 13-100 Nidzica
NIP 984-016-15-89
e-mail: sekretariat@powiatnidzicki.pl

2. Szczegółowy zakres zamówienia obejmuje:

Wspólny słownik zamówień (CPV):

- Usługi doradcze w zakresie bezpieczeństwa - 79417000-0
- Usługi opracowywania oprogramowania do zarządzania systemem - 72212781-7
- Usługi opracowywania oprogramowania informatycznego - 72212517-6
- Usługi szkoleniowe - 80500000-9

3. Opis przedmiotu zamówienia:

3.1. Przedmiotem zamówienia jest wykonanie przez zewnętrznych ekspertów usług wsparcia dotyczących projektu „Cyberbezpieczny Powiat Nidzicki (skrót CPN)” dofinansowanego z projektu z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd”

3.2. Do szczegółowych obowiązków Wykonawcy należeć będzie:

w Etapie I

1. Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji - wraz z dostarczeniem narzędzi do aktualizacji i wdrożenia SZBI dla 8 jednostek Powiatu Nidzickiego.
2. Opracowanie i wdrożenie spójnych procedur do analizy ryzyk wraz z dostarczeniem narzędzi do analizy ryzyka dla 8 jednostek PN.

w Etapie II

3. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa i SZBI dla kadry kierowniczej JST.

3.3. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji - SZBI powinna być opracowana w oparciu o wykonane analizy, Polską Normę PN-ISO/IEC 27001, ustawę o Krajowym Systemie Cyberbezpieczeństwa, dyrektywę NIS2 i Rozporządzenie Parlamentu Europejskiego RODO, ustawę o informatyzacji podmiotów realizujących zadania publiczne oraz przepisy wykonawcze.

3.4. Minimalny zakres dokumentacji SZBI zawierające niezbędne polityki i procedury, w szczególności:

1. Polityka Bezpieczeństwa Informacji;
2. Procedura zarządzania ryzykiem;
3. Instrukcja Zarządzania Systemem Informatycznym;
4. Procedury zarządzania uprawnieniami;
5. Procedura zarządzania zdalnym dostępem;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

6. Procedura szyfrowania danych;
7. Procedury zarządzania kopiami zapasowymi;
8. Polityka czystego biurka i ekranu;
9. Procedura dostępu fizycznego do pomieszczeń;
10. Procedura postępowania z incydentami bezpieczeństwa;
11. Plan ciągłości działania.

3.5. Wykonawca musi zapewnić narzędzia informatyczne w formie usługi SaaS służące do aktualizacji i wdrożenia SZBI oraz analizy ryzyka w funkcjonalności opisanej w Załączniku nr 5 - Opis funkcjonalny narzędzi informatycznych.

W ramach wsparcia dla udostępnionych narzędzi Wykonawca musi zapewnić następujące usługi:

1. Indywidualne dostosowanie narzędzi do potrzeb Zamawiającego (do 20 roboczogodzin);
2. Konsultacje techniczne realizowane przez dział wsparcia (do 20 roboczogodzin);
3. Administracje użytkownikami (do 6 roboczogodzin);
4. Szkolenia dodatkowe (do 5 roboczogodzin);
5. Automatyczny backup wykonywany codziennie (do 6 roboczogodzin);
6. Aktualizacja narzędzi do nowych przepisów (do 6 roboczogodzin);
7. Hosting w chmurze obliczeniowej (SaaS) (do 4GB HDD);
8. Bieżący serwis narzędzi informatycznych, obejmujący usuwanie błędów i usterek.

4. Wymagany termin realizacji zamówienia:

4.1. Opracowanie, uzgodnienie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji - wraz z dostarczeniem narzędzi do aktualizacji i wdrożenia SZBI dla 8 jednostek PN – **do 90 dni od podpisania umowy.**

Opracowanie i wdrożenie spójnych procedur do analizy ryzyk wraz z dostarczeniem narzędzi do analizy ryzyka dla 8 jednostek PN – **do 90 dni od podpisania umowy.**

4.2. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa i SZBI dla kadry kierowniczej JST – **do 120 dni od podpisania umowy.**

4.3. Zapewnienie usług serwisowych dla udostępnionych narzędzi informatycznych - **do dnia 20.06.2026 r.**

5. Wymagania obligatoryjne stawiane Wykonawcom

Zamawiający wymaga, aby Wykonawca spełniał następujące wymagania:

5.1. Wykonawca musi w trakcie realizacji umowy zapewnić Zespół projektowy złożony min. z 6 specjalistów:

1. Kierownik zespołu projektowego – min. 1 osoba,
2. Audytorzy bezpieczeństwa informacji – min. 3 osoby,
3. Specjalista ds. programowania – min. 1 osoba,
4. Specjalista ds. wdrożenia – min. 1 osoba,
5. Specjalista ds. technicznych – min. 1 osoba,
6. Specjalista ds. komunikacji – min. 1 osoba.

5.2. W skład zespołu projektowego muszą wchodzić osoby z następującymi certyfikatami, doświadczeniem:

- **3 audytorów bezpieczeństwa informacji**, którzy będą przeprowadzać audyt bezpieczeństwa, posiadających Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
- **2 audytorów bezpieczeństwa informacji** do opracowania planu ciągłości działania, posiadających Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;





Cyberbezpieczny Samorząd

- **1 specjalista ds. technicznych** - odpowiedzialnego za przeprowadzenie opcjonalnych testów penetracyjnych lub weryfikacji zabezpieczeń technicznych związanych z bezpieczeństwem informacji z doświadczeniem polegającym na prowadzeniu badań bezpieczeństwa w min. 5 jednostkach administracji publicznej;
 - **1 specjalista ds. wdrożenia** - odpowiedzialny za wdrażanie rozwiązań chmurowych związanych z SZBI posiadający doświadczenie polegające we wdrażaniu aplikacji chmurowych w okresie ostatnich 3 lat przed upływem terminu składania ofert w co najmniej 3 projektach dotyczących systemów informatycznych dedykowanych dla administracji publicznej;
 - **1 specjalista ds. wdrożenia** - odpowiedzialny za wdrażanie rozwiązań chmurowych związanych z SZBI posiadający doświadczenie polegające we wdrażaniu aplikacji chmurowych w okresie ostatnich 3 lat przed upływem terminu składania ofert -w co najmniej 5 projektach dotyczących systemów informatycznych dedykowanych dla administracji publicznej;
 - **1 specjalista ds. komunikacji** - odpowiedzialny za zakres koordynacji i logistyki prac zespołów projektowych posiadający doświadczenie z okresu ostatnich 3 lat przed upływem terminu składania ofert w pracy zespołowej w projektach zrealizowanych z udziałem środków zewnętrznych;
- 5.3.** Zamawiający dopuszcza łączenia funkcji, o których mowa w pkt. 5.1 i 5.2. Personel wykonawcy realizujący przedmiot zamówienia musi mieć udokumentowane i potwierdzone doświadczenie i kompetencje wykazane w **Załączniku nr 4**. - Wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia.
- 5.4.** Zamawiający wymaga, aby Wykonawca wykazał, że przeprowadził minimum 5 audytów stanu bezpieczeństwa informatycznego dla jednostek organizacyjnych administracji publicznej.
- 5.5.** Zamawiający wymaga, aby Wykonawca wykazał, że wdrożył aplikację chmurową wspomagających zarządzanie bezpieczeństwem informacji w min. w 1 JST.
- 5.6.** W celu potwierdzenia spełniania przez Wykonawcę warunków udziału w postępowaniu, Zamawiający żąda przedstawienia wykazu usług wykonanych w okresie ostatnich 5 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, daty wykonania i podmiotów, na rzecz których usługi zostały wykonane (zgodnie z **Załącznikiem nr 3** - Wykaz wykonanych usług), z załączeniem dowodów określających czy te usługi zostały wykonane należyście, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane.
- 5.7.** Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.

6. Kryteria oceny ofert :

Przy wyborze najkorzystniejszej oferty Zamawiający będzie kierował się następującymi kryteriami oceny:

A - CENA (podstawą wyliczeń będzie cena brutto)– 70% (max. 70 pkt.);

B - DOŚWIADCZENIE – 30% (max. 30 pkt.);

7. Opis sposobu przyznawania punktów.

7.1. Sposób oceny ofert w kryterium CENA:

Ilość punktów dla każdej oferty w tym kryterium zostanie wyliczona wg poniższego wzoru:

$$C = \frac{C \text{ min.}}{C \text{ bad.}} \times 70 \% \quad 1 \% - 1 \text{ punkt}$$

Gdzie:

C – ilość punktów oferty badanej

C min. – cena minimalna spośród wszystkich ofert niepodlegających odrzuceniu

C bad. – cena oferty badanej

Obliczenia dokonywane będą do dwóch miejsc po przecinku.



Cyberbezpieczny Samorząd

Maksymalnie w tym kryterium można otrzymać 70 punktów.

7.2. Sposób oceny ofert w kryterium DOŚWIADCZENIE

Doświadczenie Wykonawcy z ostatnich lat oceniane będzie zgodnie z poniższą tabelą:

| Doświadczenie | Punktacja przyznana |
|---|---------------------|
| Przeprowadzenie minimum 1 audytu stanu bezpieczeństwa informatycznego | 0 pkt |
| Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w 1 JST | 0 pkt |
| Przeprowadzenie minimum 5 audytów stanu bezpieczeństwa informatycznego dla jednostek organizacyjnych administracji publicznej | 10 pkt |
| Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w 2 JST | 10 pkt |
| Wdrożenie aplikacji chmurowych wspomagających zarządzanie bezpieczeństwem informacji w ponad 3 JST | 20 pkt |

Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w Zapytaniu ofertowym, oraz uzyska najwyższą liczbę punktów obliczoną według poniższego wzoru.

$$Pc = C + D$$

Pc – Całkowita liczba punktów uzyskanych przez badaną ofertę. C – Całkowita liczba punktów uzyskana przez badaną ofertę w kryterium „Cena”; D – Całkowita liczba punktów uzyskana przez badaną ofertę w kryterium „Doświadczenie Wykonawcy”;

Wartość punktowa zostanie podana z dokładnością do dwóch miejsc po przecinku, a zaokrąglenie zostanie dokonane zgodnie z ogólnie przyjętymi zasadami matematyki.

W przypadku, gdy oferty Wykonawców przedstawiają taki sam bilans kryterium ceny i pozostałych kryteriów, za ofertę korzystniejszą zostanie uznana oferta Wykonawcy z zaoferowaną niższą ceną.

8. Termin składania ofert:

Ofertę należy złożyć do dnia 16.05.2025 r.

poprzez stronę internetową dla systemu Baza Konkurencyjności 2021 pod linkiem

<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl>, zgodnie z Instrukcją oferenta

w BK2021 zamieszczoną na stronie internetowej, pod linkiem [https://archiwum-](https://archiwum-bazakonkurencyjnosci.funduszeuropejskie.gov.pl/info/web_instruction)

[bazakonkurencyjnosci.funduszeuropejskie.gov.pl/info/web_instruction](https://archiwum-bazakonkurencyjnosci.funduszeuropejskie.gov.pl/info/web_instruction)

9. Istotne dla zamawiającego postanowienia

9.1. Wzór umowy stanowi **załącznik nr 1** do Zapytania ofertowego otwartego.

9.2. Cenę oferty należy podać w złotych polskich z dokładnością do dwóch miejsc po przecinku zgodnie z **załącznikiem nr 2** - Formularz ofertowy. Łączna cena oferty musi obejmować cały zakres zamówienia, określony w zapytaniu ofertowym.

9.3. W cenie oferty należy uwzględnić także inne koszty o ile Oferent je przewiduje (np. koszty dojazdu, opłaty, ubezpieczenia itp.). Przy obliczaniu ceny należy uwzględnić, że cena będzie obowiązywać strony przez cały okres realizacji zamówienia. Jeżeli złożono ofertę, której wybór prowadziłoby do powstania obowiązku podatkowego Zamawiającego, zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.



Cyberbezpieczny Samorząd

10. Informacje dodatkowe:

- 10.1.** Osoba/y uprawniona/e do kontaktów:
Piotr Iwanicki, tel.: 089 625 98 27, e-mail: piotr.iwanicki@powiatnidzicki.pl,
Justyna Staniszevska Mróz, tel.: 089 625 98 36, e-mail: justyna.staniszevska.mroz@powiatnidzicki.pl
- 10.2.** Postępowanie może zostać zamknięte bez dokonania wyboru, w szczególności w przypadku, gdy oferta najkorzystniejsza, przekracza kwotę jaką Zamawiający może przeznaczyć na sfinansowanie zamówienia. Postępowanie może zostać zamknięte bez wybrania którejkolwiek oferty.
- 10.3.** Zamawiający zastrzega sobie możliwość prezentacji aplikacji do dystrybucji, aktualizacji i wdrożenia dokumentacji cyberbezpieczeństwa i analizy ryzyka.
- 10.4.** Każdy podmiot może złożyć tylko jedna ofertę.
- 10.5.** Nie dopuszcza się składania ofert wariantowych.
- 10.6.** Nie dopuszcza się składania ofert częściowych.

11. Załączniki:

- 11.1.** Załącznik nr 1 - Wzór umowy
- 11.2.** Załącznik nr 2 - Formularz ofertowy
- 11.3.** Załącznik nr 3 - Wykaz wykonanych usług
- 11.4.** Załącznik nr 4 - Wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia
- 11.5.** Załącznik nr 5 - Opis funkcjonalny narzędzi informatycznych
- 11.6.** Załącznik nr 6 - Powiązania kapitałowe
- 11.7.** Załącznik nr 7 – Zobowiązanie podmiotu udostępniającego zasoby

