

Zadanie realizowane w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020
Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU
działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia
dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

GINNA ŻYTNO
ul. Krótka 4, 97-532 Żytno
pow. radomszczański, woj. łódzkie
NIP 772-22-60-228, REGON 151398681
tel. 034/327-70-09, fax 326-90-10

Żytno, dnia 21.07.2022r.

ZPI.271.16.2022.SN

GINNA ŻYTNO OGŁASZA POSTĘPOWANIE O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO W FORMIE ZAPYTANIA OFERTOWEGO

Na zadanie pn.: „Diagnoza cyberbezpieczeństwa Urzędu Gminy Żytno do Konkursu Grantowego
Cyfrowa Gmina”

1. Nazwa i adres Zamawiającego:

Gmina Żytno, ul. Krótka 4, 97-532 Żytno

2. Określenie trybu zamówienia:

Postępowanie o udzielenie zamówienia publicznego w formie zapytania ofertowego o wartości nie
przekraczającej równowartości 130 000,00 zł.

3. Opis przedmiotu zamówienia:

Przeprowadzenie audytu cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina” Urzędu Gminy Żytno
(w dokumentacji projektu określanego jako „diagnoza cyberbezpieczeństwa”), zgodnie z zakresem oraz
formularzem stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina
zakończony raportem. Link do załącznika: „<https://www.gov.pl/attachment/d46af450-5e88-4235-825c-d6c7487d9090>”

Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem
diagnozy cyberbezpieczeństwa stanowiący załącznik nr 3 konkursu grantowego załączony do niniejszego
Zaproszenia do złożenia oferty.

4. Dane jednostki audytowej:

1. Lokalizacja jednostki audytowej (adres) – Urząd Gminy, ul. Krótka 4, 97-532 Żytno
2. Ilość pracowników/użytkowników - 19
3. Sieci:
 - 1) fizycznie separowane na poziomie UTM:
 - sieć ZYTNO.
 - 2) Wydzielona fizycznie sieć MSWiA.
4. Ilość urządzeń podłączonych do sieci ZYTNO (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki):
 - 1) komputery w sieci LAN urzędu - 21
 - 2) serwery – 1
 - 3) NAS – 1
 - 4) UTM - 1
 - 4) drukarki sieciowe - 5

- 5) routery – 1
 - 6) przełączniki "główne" - 1
 - 7) przełączniki "biurkowe" - 8
 - 8) centrala telefoniczna - 1
5. Ilość urządzeń podłączonych do sieci MSWiA:
 - 1) komputery w sieci - 2
 - 2) routery – 2
 - 3) modemy - 2
 6. Serwerownia - 1
 7. Adresy zewnętrzny - 1

5. O udzielenie niniejszego zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki:

Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Wykaz certyfikatów wskazanych w w/w rozporządzeniu:

- a) Certified Internal Auditor (CIA)
- b) Certified Information System Auditor (CISA)
- c) 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
- d) 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
- e) Certified Information Security Manager (CISM)
- f) Certified in Risk and Information Systems Control (CRISC)
- g) Certified in the Governance of Enterprise IT (CGEIT)
- h) Certified Information Systems Security Professional (CISSP)
- i) Systems Security Certified Practitioner (SSCP)
- j) Certified Reliability Professional
- k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.

6. Sposób przeprowadzenia audytu.

Zamawiający dopuszcza wykonanie audytu zdalnie w obszarach badania audytorskiego w których jest to możliwe. Badanie zabezpieczeń w tym przeprowadzenie wszelakich testów penetracyjnych sieci LAN, diagnozy cyberbezpieczeństwa, podatności systemów, wykonawca musi wykonać na miejscu w siedzibie Zamawiającego.

7. Oferta musi zawierać:

1. kompletny, wypełniony formularz ofertowy stanowiący załącznik nr 1;
2. kompletne, wypełnione oświadczenie stanowiące załącznik nr 2;
3. dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia audytu;

8. Czas realizacji, termin wykonania zamówienia:

Czas realizacji zamówienia: do 26.08.2022 r.

9. Kryteria oceny ofert:

Przy wyborze najkorzystniejszej oferty zamawiający będzie się kierował następującymi kryteriami:

- cena – 100 pkt

10. Miejsce i termin składania ofert:

Oferty należy składać w terminie do 29.07.2022r, do godz. 11:00,

1. na platformie: bazakonkurencyjnosci.funduszeuropejskie.gov.pl
2. Termin związania ofertą wynosi 30 dni.

Otwarcie ofert nastąpi w dniu 29.07.2022r. o godz. 11:30.

ZATWIERDZAM DO REALIZACJI

W O J T
mgr inż. Mirosław Ocłepa