

OR.2510.15.2022.2023

Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia dla zadania:

Przedmiotem zamówienia jest przeprowadzenie diagnozy cyberbezpieczeństwa w Konkursie Grantowym Cyfrowy Powiat oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, program Operacyjny Polska Cyfrowa na lata 2014 – 2020”

1. Przedmiotem zamówienia jest przeprowadzenie diagnozy cyberbezpieczeństwa w ramach projektu „Cyfrowy Powiat” w Starostwie Powiatowym w Tarnobrzegu **zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowy Powiat.** (stanowiącym załącznik nr 5 do opisu przedmiotu zamówienia).
2. Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (załącznik nr 5 do opisu przedmiotu zamówienia).
3. Diagnoza cyberbezpieczeństwa (audyt) musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI.
4. Diagnoza musi zostać wykonana zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowy Powiat dostępnym na stronach Centrum Projektów Polska Cyfrowa <https://www.gov.pl/web/cppc/cyfrowy-powiat> - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.
5. Wynikiem audytu jest pełny raport z przeprowadzonego audytu zawierający:
  - a. ocenę stosowanych zabezpieczeń,
  - b. analizę stanu bezpieczeństwa,
  - c. wnioski, zalecenia i rekomendację dotyczące zakresu, metodyki i organizacji zabezpieczeń.
  - d. rekomendacje dotyczące technicznych zabezpieczeń danych i informacji
6. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. 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 ww. 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)
7. Wykonawcy, którzy nie wykażą spełnienia w/w warunku udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.
8. Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
9. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).