Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 1

SR-I.042.2.4.2022

OPIS PRZEDMIOTU ZAMÓWIENIA

Wykonanie usługi audytu cyberbezpieczeństwa w ramach realizacji umowy o powierzenie grantu finansowanego w ramach projektu Cyfrowy Powiat

Zamówienia jest realizowane w ramach Umowy o powierzenie grantu o numerze 5498/P/2022 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 konkursu grantowego „Cyfrowy Powiat" o numerze POPC.05.01.00-00-0001/21-00.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego.

Jednostki samorządu terytorialnego biorące udział w projekcie „Cyfrowy Powiat" są zobowiązane do przeprowadzenia diagnozy cyberbezpieczeństwa będącej przedmiotem niniejszego zamówienia. Niezwłocznie po jej przeprowadzeniu, jej wyniki mają być przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze powyższy cel przeprowadzenia diagnozy i jej przeznaczenie.

PRZEDMIOT ZAMÓWIENIA:

1. Przedmiotem zamówienia jest wykonanie audytu (diagnozy) cyberbezpieczeństwa w Starostwie Powiatowym w Kielcach w ramach realizacji projektu zgłoszonego do Konkursu Grantowego 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.

2. Na przedmiot zamówienia składa się:
   - przeprowadzenie audytu cyberbezpieczeństwa w jednostce Zamawiającego na posiadanym przez Zamawiającego środowisku serwerowym (50 maszyn wirtualnych) oraz audyt sieci teletechnicznej;
   - przedstawienie raportu z przeprowadzonego audytu w formie papierowej i elektronicznej;
   - przekazanie wypełnionego załącznika nr 8 do Regulaminu Konkursu Grantowego Cyfrowy Powiat - „Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa" ***(załącznik nr 1 do OPZ)***.

3. Diagnoza cyberbezpieczeństwa musi uwzględniać w szczególności ocenę zgodności z:
   - Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
   - Ustawą z dnia 5 lipca 2018r o krajowym systemie cyberbezpieczeństwa.

4. Diagnoza musi być przeprowadzona:
   - w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa" stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowy Powiat. Załącznik nr 8 do Regulaminu Konkursu Grantowego opublikowany jest pod adresem: https://www.gov.pl/web/cppc/cyfrowy-powiat
     W przypadku zmiany formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa przez administratora Projektu, Wykonawca zobligowany będzie wykonać zamówienie z uwzględnieniem jego aktualnej wersji.
   - przez osoby posiadające jeden z certyfikatów uprawniających do przeprowadzeniu audytu, o których mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

   Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);
- 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;
- 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;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

5. Lokalizacja fizyczna jednostki audytowanej:
    - Starostwo Powiatowe w Kielcach, 25-211 Kielce, ul. Wrzosowa 44,
    - Filie Wydziału Komunikacji i Transportu:
        - Filia w Bielinach, ul. Partyzantów 18, 26-004 Bieliny;
        - Filia w Bodzentynie, ul. Suchedniowska 3, 26-010 Bodzentyn;
        - Filia w Chmielniku, ul. Bednarska 17, 26-020 Chmielnik;
        - Filia w Łagowie, ul. Rynek 62, 26-025 Łagów;
        - Filia w Mniowie, ul. Centralna 9, 26-080 Mniów;
        - Filia w Nowej Słupi, ul. Rynek 15, 26-006 Nowa Słupia;
        - Filia w Piekoszów, ul. Czarnowska 59, 26-065 Piekoszów;
        - Filia w Rakowie, ul. Ogrodowa 1, 26-035 Raków;
        - Filia w Strawczynie, ul. Żeromskiego 16, 26-067 Strawczyn.

6. Zamawiający nie dopuszcza wykonania diagnozy cyberbezpieczeństwa w sposób zdalny. Badanie zabezpieczeń, podatności systemów, przeprowadzenie ewentualnych testów penetracyjnych, wykonawca powinien wykonać na miejscu w siedzibie Zamawiającego.

7. Po przeprowadzeniu diagnozy, Wykonawca zobligowany jest do przekazania Zamawiającemu wypełnionego formularza diagnozy w wersji papierowej (w jednym egzemplarzu) i elektronicznej w formacie **.xlsx** lub .**xls** oraz w formacie **.pdf.**
   Wersja **.pdf** powinna być podpisana elektronicznie przez audytora wykonującego diagnozę. Formularz diagnozy musi zostać wypełniony zgodnie z zaleceniami dotyczącymi sposobu wypełniania ***załącznika nr 8*** określonymi w dokumencie „Diagnoza Cyberbezpieczeństwa – zalecenia dotyczące zasad wypełniania i wysyłania do NASK dokumentów w ramach konkursu grantowego „Cyfrowy Powiat" (***załącznik nr 2 do OPZ***).

8. W wyniku przeprowadzonego audytu i zebranych danych Wykonawca opracuje i przekaże Zamawiającemu raport wraz z oceną poziomu realizacji wymagań prawnych w zakresie bezpieczeństwa i ochrony informacji i danych oraz stanu zabezpieczeń technicznych

i organizacyjnych. Wyniki audytu opisane w raporcie powinny wskazywać możliwości rozwiązania stwierdzonych defektów i nakreślić plan działań naprawczych.

9. Zamawiający zastrzega sobie prawo do zgłaszania uwag w formie pisemnej lub drogą elektroniczną do dostarczonych przez Wykonawcę opracowań. Wykonawca zobowiązany jest do dokonania uzupełnień i poprawek w dostarczonych dokumentach w zakresie i terminie wyznaczonym przez Zamawiającego w ramach niniejszej umowy bez dodatkowego wynagrodzenia.

10. Odbiór wykonanych opracowań nastąpi na podstawie protokołu odbioru, podpisanego przez obie Strony bez zastrzeżeń, tzn. po sprawdzeniu przez Zamawiającego dostarczonych opracowań i po usunięciu przez Wykonawcę ewentualnych zgłoszonych przez Zamawiającego zastrzeżeń lub uwag. Odbiór przedmiotu zamówienia nastąpi zgodnie z procedurą opisaną w projekcie umowy.

11. Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzonej przez siebie dokumentacji na każdym etapie realizacji zamówienia oraz po jego wykonaniu, aż do zaakceptowania dokumentów przez Grantodawcę Konkursu Cyfrowy Powiat.

12. Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym kosztów ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku i skanu dokumentów.

13. W ramach wynagrodzenia za realizacje usługi Wykonawca przeniesie na całość autorskich praw majątkowych oraz prawo zezwalania na wykonywanie zależnych praw autorskich do wykonanej dokumentacji. Nabycie praw autorskich następuje bez ograniczeń czasowych i terytorialnych, na wszystkich znanych polach eksploatacji, a w szczególności:
    - utrwalania jakąkolwiek techniką, zwielokrotniania dokumentacji, będącej wynikiem realizacji umowy, w całości lub części, dowolną techniką w nieograniczonej liczbie egzemplarzy,
    - publicznego prezentowania, odtwarzania za pomocą dowolnych środków technicznych, wprowadzania do sieci teleinformatycznej Zamawiającego lub innych serwisów, w których takie udostępnienie będzie obligatoryjne lub niezbędne,
    - wprowadzenie do pamięci komputera i sporządzanie kopii dla celów eksploatacji, trwałe i czasowe zwielokrotnianie zapisu wszelkimi dostępnymi środkami i sposobami,
    - rozpowszechniania i wprowadzenia do obrotu, elektroniczne udostępnienie upoważnionym osobom,
    - przekazywanie lub przesyłanie zapisów utworów pomiędzy komputerami, serwerami i użytkownikami, innymi odbiorcami, przy pomocy wszelkiego rodzaju środków i technik,
    - publiczne wykorzystanie w materiałach informacyjnych, wydawniczych,
    - wykorzystanie w inny sposób w związku z realizacją umowy o powierzenie grantu, w ramach której realizowany jest przedmiot zamówienia.

Równolegle z nabyciem autorskich praw majątkowych, Zamawiający nabywa własność wszystkich egzemplarzy dokumentacji wykonanej przez Wykonawcę.

14. Zamawiający udostępni Wykonawcy wszelkie informacje, dane i dokumenty wewnętrzne Zamawiającego niezbędne do prawidłowego wykonania przedmiotu umowy.

15. Wykonawca zobowiązany jest do zachowania poufności oraz nie udostępniania osobom trzecim, w tym także nieupoważnionym pracownikom, informacji i danych, które uzyskał w trakcie lub w związku z realizacją przedmiotu zamówienia, o ile informacje takie nie są powszechnie znane, bądź obowiązek ich ujawnienia nie wynika z obowiązujących przepisów, orzeczeń sądowych lub decyzji odpowiednich władz.

Termin wykonania zamówienia: do 40 dni od dnia zawarcia umowy.

Kryteria oceny ofert – cena 100%