Zamówienie współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, 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 o numerze POPC.05.01.00-00-0001/21-00.

Zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych – część 1.

Diagnoza cyberbezpieczeństwa w Gminie Grzegorzew w projekcie Cyfrowa Gmina w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczącego realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

1. Przedmiotem zamówienia jest przeprowadzenie audytu cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina” w Urzędzie Gminy w Grzegorzewie (w dokumentacji projektu określana jako „diagnoza cyberbezpieczeństwa”) zgodnie z zakresem określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa” stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego „Cyfrowa Gmina”.
2. Przeprowadzenie diagnozy cyberbezpieczeństwa musi zostać wykonane 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 2012r. 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, w tym opracowanie raportu zawierającego wnioski i rekomendacje.
3. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 1, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia o których mowa w dokumentach zamówienia.
4. Wykonawca przedstawi wynik testów w postaci raportu zawierającego zestawienie sprawdzeń oraz zestawu zaleceń umożliwiających minimalizację zidentyfikowanych ryzyk.
5. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowej diagnozy/audytu bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu (w tym w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów elektronicznych, analizy zewnętrznej i wewnętrznej sieci komputerowej, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy poczty email, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w podmiocie) oraz opracowania dokumentacji po audytowej – raportu z wytycznymi do doskonalenia i rekomendacjami.
6. Jednostki samorządu terytorialnego biorące udział w projekcie „Cyfrowa Gmina” 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.

7. Wykonawca wskaże obszary szczególnie podatne na zagrożenia teleinformatyczne i poda Zamawiającemu sugestie ich wyeliminowania.
8. Diagnoza zostanie przeprowadzona w zakresie dwóch lokalizacji w budynkach Urzędu Gminy w Grzegorzewie (Plac 1000-lecia Państwa Polskiego 1 oraz Plac 1000-lecia Państwa Polskiego 6)
    a. W infrastrukturze teleinformatycznej Urzędu Gminy znajduje się 22 aktywnych użytkowników.
    b. Ilość komputerów objętych diagnozą: 28
    c. Ilość serwerów fizycznych objętych diagnozą: 1
    d. W sieciach zamawiającego występują dwa adresy IP (zewnętrzne)
    e. Ilość podsieci objętych diagnozą: 2
    f. Brak AD.
9. W związku z rozległym zakresem zamówienia Zamawiający nie przewiduje możliwości wykonania zadania za pomocą technik dostępu zdalnego. Dokumentacja w formie papierowej znajdująca się na stanowiskach nie posiada postaci elektronicznej. Konieczna obecność fizyczna w jednostce zamawiającego podczas wykonywania zamówienia.