15 lipca 2024

Zwiększenie poziomu bezpieczeństwa informacji w Urzędzie Gminy Korzenna

Projekt współfinansowany przez Unię Europejską w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

Tytuł projektu: „Zwiększenie poziomu bezpieczeństwa informacji w Urzędzie Gminy Korzenna"

Okres realizacji: 27.06.2024 r. – 27.06.2026 r.

Beneficjent: Gmina Korzenna

Całkowity koszt zadania wg wniosku o dofinansowanie (koszt netto): 850 000,00 zł

Kwota dofinansowania: 850 000,00 zł (współfinansowanie UE **ze środków FERC 81%:** 688 500,00 zł, Budżet Państwa BP 19%: 161 500,00 zł

Wkład własny Gminy Korzenna: obejmuje podatek VAT

Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1365/ FERC.02.02-CS.01-001/23/2024

Cel projektu:

Celem Projektu grantowego jest wsparcie JST w zakresie realizacji usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji jednostki samorządu terytorialnego.

Realizacja projektu poprzez wsparcie grantowe jednostki samorządowej, przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI),
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu

widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

<u>Krótki opis zakresu rzeczowego projektu:</u>

Gmina Korzenna otrzymała grant w wysokości 850 000,00 zł, a uzyskane środki będzie mogła wykorzystać w następujących obszarach:

1. **obszar organizacyjny** – środki można przeznaczyć na następujące działania (usługi):
    a. opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym między innymi wprowadzenie lub aktualizacja polityk bezpieczeństwa informacji (PBI), na analizy ryzyka (w tym opracowanie i wdrożenie metodyk), np. procedury: obsługi incydentów, ciągłości działania i zarządzania kryzysowego, stosowania kryptografii i szyfrowania, kontroli dostępu, bezpieczeństwa pracy zdalnej, używania urządzeń mobilnych, itp.,
    b. audyt SZBI, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów, (re-)certyfikacja SZBI na zgodność z normami;
2. **obszar kompetencyjny** – środki można przeznaczyć na następujące działania (usługi):
    a. podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST,
    b. szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji,
    c. szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu,
    d. szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami;
3. **obszar techniczny** – środki można przeznaczyć na następujące działania (usługi):
    a. zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta,
    b. zakup, wdrożenie i utrzymanie rozwiązań ciągłego monitorowania bezpieczeństwa, skanery podatności, zarządzanie podatnościami, zarządzanie zasobami IT i aktywami podlegającymi ochronie oraz innych rodzajów narzędzi wymienionych poniżej w katalogu klas rozwiązań,
    c. zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa,

d. zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa,
e. zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych,
f. zakup testów i badań bezpieczeństwa, dostępu do informacji bezpieczeństwa (np. ang. feeds) oraz inne usługi integracyjne dotyczące obszaru cyberbezpieczeństwa

Grupa docelowa:

Grupą docelową projektu jest administracja publiczna: jednostka samorządu terytorialnego (JST)

#FunduszeUE

#FunduszeEuropejskie