

Systemowy identyfikator wniosku

0a1e6d09-c5b4-449c-9c99-a7e213fce842

1. Informacje ogólne o projekcie

| | |
|-----------------------|--|
| Data złożenia wniosku | 2023-12-14 10:42:22 |
| Program | Fundusze Europejskie na Rozwój Cyfrowy (FERC) |
| Priorytet | II Zaawansowane usługi cyfrowe |
| Działanie | 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa |
| Fundusz | Europejski Fundusz Rozwoju Regionalnego (EFRR) |
| Numer naboru | FERC.02.02-CS.01-001/23 |
| Tytuł projektu | Cyberbezpieczny Samorząd Gminy Daleszyce |
| | <p>Projekt ma na celu zwiększenie poziomu bezpieczeństwa informacji w Urzędzie Miasta i Gminy Daleszyce i w 6 jednostkach podległych (ZSP, MGŻ, SP w Mójczy, SP w Niestachowie, SP w Sukowie, MGOPS) poprzez wzmacnianie odporności na zagrożenia w cyberprzestrzeni oraz zdolność do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych.</p> <p>W tym celu z uwzględnieniem posiadanej infrastruktury IT oraz posiłkując się doradztwem firmy zewnętrznej w określeniu potrzeb i doboru odpowiednich rozwiązań w zakresie wzmocnienia cyberbezp. w ramach konkursu zaplanowano szereg działań wzmacniających odporność cybernetyczną :</p> <p>W obszarze organizacyjnym: Skorzystanie z zewnętrznych usług doradczych w fazie aplikowania o grant co już powyżej zostało ujęte a także podczas jego realizacji, aby wspierać się fachową wiedzą i doświadczeniem min. podczas postępowań zakupowych, aby zostały przeprowadzone zgodnie prawem i regulaminem konkursu a specyfikacja planowanych zakupów sprzętu, oprogramowania, czy wdrażanych usług, szkoleń zwiększających cyberbezp. została sprecyzowana zgodnie z zaplanowanym przeznaczeniem. W urzędzie i w jednostkach podległych planujemy przeprowadzić przegląd, aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) a w przypadku jej nieposiadania lub posiadania niekompletnej opracowanie i wdrożenie, które polegać będzie na dostosowaniu zakresu dokumentacji do normy ISO 27001 a także wprowadzeniu lub aktualizacji polityk bezpieczeństwa informacji (PBI), procedur i instrukcji np: obsługi incydentów, ciągłości działania, stosowania kryptografii i szyfrowania, kontroli dostępu. Przeprowadzenie audytu SZBI i audytu zgodności KRI przez wykwalifikowanych audytorów na zakończenie projektu w urzędzie i jednostkach podległych.</p> <p>W obszarze technicznym: w ramach konkursu grantowego planowany jest zakup sprzętu, oprogramowania i usług zwiększających cyberbezp. w urzędzie i w jednostkach podległych. Szczegóły zakupu sprzętu i oprogramowania jest ujęty we wniosku.</p> <p>W obszarze kompetencyjnym: zaplanowano szkolenia, ramach monitorowania utrzymania efektów projektu tj. utrzymania środków trwałych i usług nabytych w ramach Projektu opracuje i wprowadzi odpowiednie procedury monitorowania w tym zakresie.</p> <p>Celem projektu jest wsparcie w zakresie podwyższenia poziomu bezpieczeństwa w zakresie realizacji usług publicznych w obszarze teleinformatycznym, poprzez zwiększenie cyfryzacji jednostki samorządu terytorialnego wraz z jednostkami podległymi w kontekście zwiększenia poziomu cyberbezp. .</p> <p>Projekt przewiduje dostosowanie struktury informatycznej GD i</p> |



Koncepcja realizacji

jednostek podległych biorących udział w projekcie poprzez opracowanie i wdrożenie dokumentów SZBI, przeprowadzenie audytu zgodnie z KRI oraz ankiety dojrzałości oraz zakup i wdrożenie urządzeń i oprogramowania. Projekt ten jest zgodny z celem szczegółowym. Działania FERC.02.02 Wzmocnienie krajowego systemu cyberbezpieczeństwa, co ma na celu wykorzystanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych. Analiza stanu aktualnego w zakresie infrastruktury i systemów IT wskazuje na następujące potrzeby:

- Wsparcie merytoryczne projektu(W1)P: UMiG, ZSP, MGŻ, SP w Mójczy, SP w Niestachowie, SP w Sukowie, MGOPS
- Audyt końcowy projektu(W2) P: UMiG, ZSP, MGŻ, SP w Mójczy, SP w Niestachowie, SP w Sukowie, MGOPS
- System Zarządzania Bezpieczeństwem Informacji (W3) P: UMiG, ZSP, MGŻ, SP w Mójczy, SP w Niestachowie, SP w Sukowie, MGOPS
- Oprogramowanie antywirusowe(W4) U: zapewni ciągłość ochrony antywirusowej, kluczowej dla zapobiegania atakom złośliwego oprogramowania. Oprogramowanie oferuje zaawansowane funkcje bezpieczeństwa i regularne aktualizacje, podnosząc poziom ochrony danych i prywatności użytkowników. P: UMiG, ZSP, MGŻ, SP w Mójczy, SP w Niestachowie, SP w Sukowie, MGOPS
- System monitorowania i zdalnego zarządzania urządzeniami sieciowymi (W5) U: Wdrożenie systemu umożliwi ciągłe śledzenie stanu sieci, wykrywanie nieprawidłowości oraz szybką reakcję na potencjalne zagrożenia. Taki system zapewnia również efektywniejsze zarządzanie zasobami sieciowymi, co jest kluczowe dla utrzymania bezpieczeństwa, wydajności i dostępności krytycznych usług komunalnych w obliczu rosnących wyzwań cybernetycznych. P: UMiG
- Update licencji serwerowej (W9) U: Zwiększy bezpieczeństwo sieci poprzez regularny dostęp do najnowszych funkcji zabezpieczeń i wsparcia technicznego od Microsoft. Na systemie serwerowym będzie zainstalowane oprogramowanie do Backup w celu podniesienia poziomu cyberbezpieczeństwa P: UMiG
- Oprogramowanie do analizy sieci IT (W10) U: Wdrożenie pozwoli to na natych. identyfikację niezwykłych lub potencjalnie szkodliwych aktywności w infrastrukturze IT. Dzięki ciągłemu monitorowaniu możliwe jest szybkie wykrywanie ataków, awarii lub anomalii. Ponadto, takie narzędzia umożliwiają gminie skuteczne zarządzanie swoją infrastrukturą, co jest kluczowe dla utrzymania ciągłości działania oraz ochrony przed cyberatakami. P: UMiG
- Dyski do serwera NAS(W16) U: W celu zapobieżenia utracie danych niezbędne jest zastosowanie systemu kopii zapasowych.P: UMiG
- Serwer kopii bezpieczeństwa(W16) U: Brak centralnego systemu tworzenia kopii zapasowych dla komp. zarządu. Obecnie kopia zapasowa baz danych jest tworzona lokalnie na dysku USB co jest niewystarczające i naraża jednostkę na ryzyko. Potrzebny jest zakup serwera do tworzenia kopii zapasowych i konfiguracja zdalnych kopii zapasowych na serwerze Synology UMiG, co zapewni dodatkową warstwę ochrony. P:UMiG
- UPSy do stacji roboczych(W16) U: UPS pozwalają na ciągłą pracę w przypadku awarii zasilania. Daje to czas na bezpieczne wyłączenie sprzętu lub przełączenie na generator zasilania w przypadku dłuższych przerw w dostawie energii. P: UMiG, ZSP, MGŻ, SP w Mójczy, SP w Niestachowie, SP w Sukowie, MGOPS
- System do gromadzenia logów(W8) U: Wdrożenie systemu zgodnego z KRI par.21 pozwala na szczegółową analizę aktywności w sieci, co jest kluczowe dla wczesnego wykrywania i reagowania na potencjalne zagrożenia. Dzięki temu, organizacja może szybciej identyfikować i neutralizować cyberataki.P: UMiG

- Switch zarządzany(W8) U: Te urządzenia zapewnią większą przepustowość, elastyczność i możliwość zdalnego zarządzania, co poprawi wydajność i bezpieczeństwo sieci. P: UMiG, MGOPS

- UPSy do serwerów(W16) U: który jest urządzeniem mającym na celu zapewnienie zasilania awaryjnego w przypadku utraty zasilania elektrycznego. UPS jest istotnym elementem w ochronie serwerów i sprzętu komp. przed nagłymi przerwami w dostawie prądu. P: UMiG

- Macierz dyskowa(W28)U: Aktualnie brak jest dedykowanej macierzy do przech. danych maszyn wirtualnych. Macierz pełni kluczową rolę w zapewnieniu wydajności, niezawodności i skalowalności infrastruktury wirtualnej. P: UMiG

- Urządzenia UTM(W4)U: Jednostki nie posiadają zaawansowanej zapory sieciowej (firewall) z funkcją Unified Threat Management (UTM), która oferuje aktywne skanowanie ruchu sieciowego w celu wykrywania i blokowania zagrożeń. Dla lepszego zabezpieczenia sieci proponuje się wprowadzenie zaawansowanej zapory sieciowej z funkcją UTM. P: UMiG, MGOPS

- Centralne zarządzanie punktem dostępu(W4) U: Aktualnie brak centralnego zarządzanego systemu punktów dostępu. Aby poprawić wydajność i bezpieczeństwo sieci Wi-Fi, proponuje się wdrożenie systemu centralnego zarządzania punktami dostępowymi. P: UMiG

- Szkolenia kadry zarządzającej i informatyków (W11) U: Szkolenie z zakresu cyberbezp. znacząco podnosi ich świadomość dotyczącą potencjalnych zagrożeń cyfrowych, co przyczynia się do lepszego rozpoznawania i zapobiegania cyberatakam. Takie szkolenie zwiększa kompetencje pracowników w zakresie stosowania najlepszych praktyk i procedur bezpieczeństwa, co bezpośrednio wpływa na ochronę infrastruktury informatycznej i danych mieszkańców. P: UMiG

- Szkolenia pracowników(W11) U: Pracownicy JST, dzięki szkoleniom z cyberbezp. , stają się bardziej świadomi potencjalnych cyberzagrożeń. To zwiększa ich zdolność do ochrony kluczowych zasobów gminy. P: UMiG

- Usługa skanowanie podatności infrastruktury IT(W4) U: Regularne skanowanie sieci, umożliwia wczesne wykrywanie i łatanie luk w zabezpieczeniach, co znacząco zmniejsza ryzyko ataków cybernetycznych. Jest to kluczowe dla utrzymania zgodności z przepisami dotyczącymi bezpieczeństwa danych. Automatyzacja tego procesu oszczędza czas i zasoby, co przekłada się na efektywniejsze zarządzanie bezpieczeństwem IT w organizacji. P: UMiG

- Wsparcie przy wdrożeniu sprzętu IT (W16) U: Nowy sprzęt pozwala na efektywniejsze wykrywanie i neutralizowanie zagrożeń, co jest kluczowe dla ochrony przed zaawansowanymi atakami cybernetycznymi. Dzięki temu organizacja jest lepiej przygotowana na różnorodne scenariusze zagrożeń. P: UMiG

- Szkolenie z oprogramowania do analizy sieci IT(W19) U: Szkolenie z oprogramowania umożliwiającego automatyczne wykrywanie sieci i monitorowanie serwerów, aplikacji, serwisów i urządzeń pozwala informatykom na lepsze zrozumienie możliwości tego narzędzia w monitorowaniu infrastruktury IT i sieci. Dzięki temu mogą efektywniej wykrywać i reagować na potencjalne zagrożenia w czasie rzeczywistym. P: UMiG

- Wsparcie przy wdrożeniu systemów kopii bezpieczeństwa(W16) U: Wdrożenie systemów backupu danych zgodnie z zasadą 3-2-1 pod backup zapewnia niezawodne zabezpieczenie danych, minimalizując ryzyko utraty informacji w przypadku awarii systemu. Ta metoda zapewnia zróżnicowanie kopii zapasowych, co jest kluczowe dla ochrony przed różnorodnymi scenariuszami zagrożeń. P: UMiG

Na każdym etapie realizacji projektu Wnioskodawca nadrzędnie dążyć będzie do zagwarantowania, aby projekt był dostępny dla każdego uczestnika, niezależnie bez względu na płeć, wiek, niepełnosprawność,

| | |
|------------------|--|
| | rasę lub pochodzenie etniczne, wyznawaną religię lub światopogląd, orientację seksualną. |
| Projekt grantowy | Tak |

2. Miejsce realizacji projektu

| | |
|---|-----------------------------------|
| Obszar realizacji projektu (TERYT) | 2604053 |
| Maksymalna kwota dofinansowania grantu dla Beneficjenta (liczona po współczynniku dochodów Beneficjenta (w PLN) | 850000,00 |
| Minimalna wysokość wkładu własnego (wyrażona w %) | 8,00 |
| Procent dofinansowania UE (w %) | 77,28 |
| Procent dofinansowania BP (w %) | 14,72 |
| Województwo/Powiat/Gmina | ŚWIĘTOKRZYSKIE/kielecki/Daleszyce |

3. Informacje o Grantobiorcy

| | |
|---------------------------|-----------------------|
| NIP | 6572525617 |
| Nazwa Grantobiorcy | GMINA DALESZYCE |
| Regon | 291010040 |
| KRS | <i>brak danych</i> |
| Forma Prawna Grantobiorcy | WSPÓLNOTY SAMORZĄDOWE |
| Możliwość odzyskania VAT | Nie |

Adres siedziby

| | |
|-------------------------|------------------------|
| Kraj | Polska |
| Miejscowość | Daleszyce |
| Kod pocztowy | 26-021 |
| Ulica | pl. Staszica |
| Nr domu | 9 |
| Nr lokalu (opcjonalnie) | <i>nie dotyczy</i> |
| Adres e-mail | gmina@daleszyce.pl |
| Adres ePUAP | /d50r93xsl6/SkrytkaESP |
| Nr tel | +48 413171694 |

Adres korespondencyjny

| | |
|---|-----|
| Adres korespondencyjny taki sam jak adres firmy | tak |
|---|-----|

Osoba upoważniona do kontaktu

| | |
|----------|---------|
| Imię | Anna |
| Nazwisko | Kosmala |

| | |
|------------------------------------|--|
| Stanowisko | Kierownik Wydziału Administracji i Rozwoju |
| Adres e-mail | anna.kosmala@daleszyce.pl |
| Nr tel | +48 413171694 |
| Nr rachunku bankowego Grantobiorcy | 45 8485 0009 0000 0130 2000 0184 |

Osoby upoważnione do reprezentacji Grantobiorcy

| | |
|---------------------|------------------------------------|
| Imię | Dariusz |
| Nazwisko | Meresiński |
| Stanowisko | Burmistrz Miasta i Gminy Daleszyce |
| Podpis/kontrasynata | podpis |
| Adres e-mail | dariusz.meresinski@daleszyce.pl |
| Nr tel | +48 413171694 |

| | |
|---------------------|-----------------------------------|
| Imię | Ilona |
| Nazwisko | Piwowska |
| Stanowisko | Skarbnik Miasta i Gminy Daleszyce |
| Podpis/kontrasynata | kontrasynata |
| Adres e-mail | ilona.piwowska@daleszyce.pl |
| Nr tel | +48 413171694 |

4. Zakres rzeczowy projektu

Zadanie

| | |
|---------------|----------------------|
| Nazwa zadania | Obszar organizacyjny |
|---------------|----------------------|

Zadanie

| | |
|---------------|-------------------|
| Nazwa zadania | Obszar techniczny |
|---------------|-------------------|

Zadanie

| | |
|---------------|----------------------|
| Nazwa zadania | Obszar kompetencyjny |
|---------------|----------------------|

5. Zakres finansowy

Wydatki rzeczywiście ponoszone

Zadanie 1 - Obszar organizacyjny

| Lp. | Nazwa kosztu | Cena jednostkowa (w PLN) | Liczba jednostek | Wydatki ogółem (w PLN) | Wydatki kwalifikowalne (w PLN) | Wydatki niekwalifikowalne (w PLN) | Dofinansowanie (w PLN) | Wkład własny (w PLN) |
|-----|--------------------------------|--------------------------|------------------|------------------------|--------------------------------|-----------------------------------|------------------------|----------------------|
| 1 | Wsparcie merytoryczne projektu | | | | | | | |

| | | | | | | | | |
|---|---|--|------|--|--|--|--|--|
| 2 | Audyt końcowy projektu | | | | | | | |
| 3 | System Zarządzania Bezpieczeństwem Informacji | | | | | | | |
| | | | SUMA | | | | | |

Zadanie 2 - Obszar techniczny

| Lp. | Nazwa kosztu | Cena jednostkowa (w PLN) | Liczba jednostek | Wydatki ogółem (w PLN) | Wydatki kwalifikowalne (w PLN) | Wydatki niekwalifikowalne (w PLN) | Dofinansowanie (w PLN) | Wkład własny (w PLN) |
|-----|---|--------------------------|------------------|------------------------|--------------------------------|-----------------------------------|------------------------|----------------------|
| 1 | Oprogramowanie antywirusowe | | | | | | | |
| 2 | System monitorowania i zdalnego zarządzania urządzeń sieciowych | | | | | | | |
| 3 | UPSy do serwerów | | | | | | | |
| 4 | Update licencji serwerowej | | | | | | | |
| 5 | Oprogramowanie do analizy sieci IT | | | | | | | |
| 6 | Dyski do serwera NAS | | | | | | | |
| 7 | serwer do kopii bezpieczeństwa wraz z dyskami | | | | | | | |
| 8 | UPSy do stacji roboczych | | | | | | | |
| 9 | System do gromadzenia logów | | | | | | | |
| 10 | Switch zarządzany | | | | | | | |
| 11 | Macierz dyskowa | | | | | | | |
| 12 | Urządzenia UTM | | | | | | | |



| | | | | | | | | |
|----|---------------------------------------|--|--|--|--|--|--|--|
| 13 | Centralne zarządzanie punktem dostępu | | | | | | | |
| | | | | | | | | |

Zadanie 3 - Obszar kompetencyjny

| Lp. | Nazwa kosztu | Cena jednostkowa (w PLN) | Liczba jednostek | Wydatki ogółem (w PLN) | Wydatki kwalifikowalne (w PLN) | Wydatki niekwalifikowalne (w PLN) | Dofinansowanie (w PLN) | Wkład własny (w PLN) |
|-----|---|--------------------------|------------------|------------------------|--------------------------------|-----------------------------------|------------------------|----------------------|
| 1 | Szkolenia kadry zarządzającej i informatyk | | | | | | | |
| 2 | Szkolenia pracowników | | | | | | | |
| 3 | Usługa skanowanie podatności infrastruktury IT | | | | | | | |
| 4 | Wsparcie przy wdrożeniu sprzętu IT | | | | | | | |
| 5 | Szkolenie z oprogramowania do analizy sieci IT | | | | | | | |
| 6 | Wsparcie przy wdrożeniu systemów kopii bezpieczeństwa | | | | | | | |
| | | | SUMA | | | | | |

Ogółem wydatki rzeczywiście ponoszone

| Ogółem wydatki rzeczywiście ponoszone | Wydatki ogółem (w PLN) | Wydatki kwalifikowalne (w PLN) | Wydatki niekwalifikowalne (w PLN) | Dofinansowanie (w PLN) | Wkład własny (w PLN) |
|---------------------------------------|------------------------|--------------------------------|-----------------------------------|------------------------|----------------------|
| Wszyscy - ogółem | 923 913,00 | 923 913,00 | 0,00 | 849 999,98 | 73 913,02 |

Podsumowanie budżetu

| | Wydatki ogółem (w PLN) | Wydatki kwalifikowalne (w PLN) | Dofinansowanie (w PLN) |
|-------------------|------------------------|--------------------------------|------------------------|
| Razem w projekcie | 923 913,00 | 923 913,00 | 849 999,98 |

6. Montaż finansowy

| Wydatki ogółem | Wydatki kwalifikowalne | Dofinansowanie | Procent dofinansowania | Wkład UE | Procent dofinansowania UE | Procent dofinansowania BP | Wkład BP | Wkład własny z wydatków ogółem | Wkład własny z wydatków kwalifikowalnych | Procent wkładu własnego kwalifikowalnego |
|----------------|------------------------|----------------|------------------------|------------|---------------------------|---------------------------|------------|--------------------------------|--|--|
| 923 913,00 | 923 913,00 | 849 999,98 | 92,00 | 714 000,00 | 77,28 | 14,72 | 136 000,00 | 73 913,02 | 73 913,02 | 8,00 |

7. Źródła finansowania wydatków (w PLN)

| | Wydatki ogółem | Wydatki kwalifikowalne |
|---|----------------|------------------------|
| Dofinansowanie | 849 999,98 | 849 999,98 |
| Razem wkład własny: | 73 913,02 | 73 913,02 |
| Budżet państwa | 0,00 | 0,00 |
| Budżet Jednostek Samorządu Terytorialnego | 73 913,02 | 73 913,02 |
| Inne publiczne | 0,00 | 0,00 |
| Prywatne | 0,00 | 0,00 |
| SUMA | 923 913,00 | 923 913,00 |

8. Oświadczenia i załączniki

Oświadczenia

Pouczony(-a) o odpowiedzialności za składanie oświadczeń niezgodnych z prawdą, w tym o konieczności zwrotu przyznanego w ramach projektu „Cyberbezpieczny Samorząd” wsparcia

| | |
|--|-------------------------------------|
| Oświadczam, że w przypadku projektu nie nastąpiło, nie następuje i nie nastąpi nakładanie się finansowania przyznanego z funduszy strukturalnych Unii Europejskiej, Funduszu Spójności lub innych funduszy, programów, środków i instrumentów finansowych Unii Europejskiej ani krajowych środków publicznych, a także z państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA). | <input checked="" type="checkbox"/> |
| Oświadczam, że zapoznałem się/zapoznałam się z Regulaminem naboru i akceptuję jego zasady. | <input checked="" type="checkbox"/> |
| Oświadczam, że nie podlegam wykluczeniu z możliwości otrzymania dofinansowania ze środków UE. | <input checked="" type="checkbox"/> |
| Oświadczam, że podane przeze mnie dane w Formularzu Aplikacyjnym o grant i złożone oświadczenia są prawdziwe. | <input checked="" type="checkbox"/> |
| Zobowiązuję się, w przypadku pozytywnego rozpatrzenia mojego wniosku, do przesłania dokumentów potwierdzających upoważnienie do reprezentacji dla osób podpisujących umowę grantową. | <input checked="" type="checkbox"/> |

| | |
|---|-------------------------------------|
| Oświadczam, że zapoznałem/am się i akceptuję warunki Kompletnego Schematu Grantowego w projekcie "Cyberbezpieczny Samorząd" i zobowiązuję się do jego przestrzegania. | <input checked="" type="checkbox"/> |
| Oświadczam, że przestrzegam przepisów dotyczących zasad horyzontalnych, o których mowa w art. 9 lub motywie 6 rozporządzenia nr 2021/1060. | <input checked="" type="checkbox"/> |
| Oświadczam, że nie podlegam pomocy publicznej nie otrzymałem/łam pomocy de minimis na przedsięwzięcie, na którego realizację złożony został wniosek o dofinansowanie. | <input checked="" type="checkbox"/> |

Załączniki

Dokumenty potwierdzające prawo do reprezentacji Grantobiorcy

| Nazwa | Rozmiar | Suma kontrolna |
|---|---------|--|
| + Zaświadczenie - powołanie skarbnika bez zgodności-sig.pdf | 771 KB | 460a361fa90079008bfe1a6c5937f29a3dc0d6a186d8d2eece4c932298ad9625 |

Oświadczenie Grantobiorcy dot. VAT

| Nazwa | Rozmiar | Suma kontrolna |
|---|---------|--|
| Załącznik_nr_7_-_Oświadczenie_dotyczące_kwalifikowalności_podatku_VAT-sig.pdf | 345 KB | 9984169bf85f24d9d321a3dc972659cb6b4548149c2329a9ad74b1062ee5b05f |

Dodatkowe dokumenty ze strony Grantobiorcy

| Nazwa | Rozmiar | Suma kontrolna |
|---------------------------------|---------|---|
| uchwały i statuty jednostek.zip | 11 MB | 2e7743aa154a4e1cbbcd054b4c594bb5d2c075a3f536edd6f9d12c6f8618857 |