Systemowy identyfikator wniosku	c20fc03f-2385-4089-898e-ddb4a9a6efab

1. Informacje ogólne o projekcie

Data złożenia wniosku	2023-12-14 13:02:04
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	Zwiększenie cyberbezpieczeństwa Urzędu Gminy Lesznowola
	Celem projektu jest zwiększenie poziomu bezpieczeństwa informacji UG Lesznowola. Projekt realizuje cel szczegółowy Programu FERC2021 /2027, Działanie 2.2 Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa w zakresie zapewnienia cyberbezpieczeństwa jednostkom administracji publicznej poprzez budowę, rozwój oraz wdrażanie narzędzi służących do monitorowania bezpieczeństwa, zbierania, analizy i wymiany informacji o zagrożeniach, podatnościach i incydentach, a także poprzez rozwój cyfrowych kompetencji pracowników w obszarze cyberbezpieczeństwa. Koncepcja projektu opracowana została na podstawie analizy potrzeb jednostki w zakresie cyberbezpieczeństwa w obszarze organizacyjnym, kompetencyjnym oraz technicznym w oparciu o posiadaną dokumentację, opracowaną Ankietę Dojrzałości Cyberbezpieczeństwa, badanie stanu infrastruktury technicznej oraz kompetencji pracowników i kadry kierowniczej w zakresie cyberbezpieczeństwa. Zakres projektu oraz rozwiązania w nim zastosowane zostały opracowane w oparciu o Poradnik Cyberbezpieczny Samorząd. Okres realizacji projektu wyniesie 24 miesiące od podpisania umowy grantowej. Zadanie 1. Obszar organizacyjny. Przeprowadzona analiza dojrzałości cyberbezpieczeństwa wykazała, że Gmina posiada luki w obszarze organizacyjnym polegające przede wszystkim na braku aktualizacji całościowego SZBI, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki Bezpieczeństwa Informacji w/w dokumenty nie były aktualizowane od 2018 roku i opisują procedury oraz środki techniczne i organizacyjne zapewniające ochronę danych bez uwzględnienia zmian z zakresu cyberbezpieczeństwa. W ramach projektu zaplanowano aktualizację i wdrożenie całościowego SZBI (W.01), w ramach którego opracowana zostanie kompleksowa Polityka Bezpieczeństwa Informacji (W.14) uwzględniająca cały obszar ochrony informacji, łącznie z obszarem dotyczącym cyberbezpieczeństwa. W związku z tym, w projekcie zaplanowano przeprowadzenie przeglądu zgodności polityk z KRI i UoKSC (W.02) oraz wykonanie testów podatnościowych (W.02, W.04, W.14, W.17), które będą podstawą do opracowania procedur identyfikacji i zarządzania podatnościami, także w kontekście cyberbezpieczeństwa (W.20, W.21). W projekcie przewidziano przeprowadzenie analizy ryzyka, której wyniki stanowić będą bazę do opracowania pełnego, uwzględniającego obszar cyberbezpieczeństwa rejestru ryzyk oraz procedur zarządzania nimi (W. 04). Zaktualizowany rejestr ryzyk obejmować będzie wszystkie, także informatyczne aktywa jednostki (W.03). W zakresie ochrony danych, opracowane zostaną procedury uwzględniające cyberbezpieczeństwo (W.17), w tym bezpieczeństwo kopii zapasowych (W.19) oraz plany ich

Koncepcja realizacji	odtwarzania w przypadku awarii (W.16). Zaktualizowane SZBI regulować będzie także procedury związane z rejestrowaniem i przechowywaniem logów oraz informacji o anomaliach i zdarzeniach (W.08, W.25, W.26, W. 27, W.28), a także procedury związane z obsługą incydentów (W.04, W. 21, W.23, W.29, W.30, W.31). Na zakończenie projektu przewidziano wykonanie audytu powdrożeniowego wraz z raportem (W.24). Powyższe zadania zrealizowane zostaną z wykorzystaniem podmiotów zewnętrznych (W. 02) posiadających odpowiednie doświadczenie oraz kwalifikacje. W zakresie organizacyjnym przewidziano przeprowadzenie działań promocyjnych zgodnie z wymaganiami ustawowymi oraz zapisami Umowy o Powierzenie Grantu (W.34). Koszty usług oszacowano na podstawie dostępnych na rynku ofert. Zadanie 2. Obszar kompetencyjny. Aktualnie, pracownicy Urzędu nie są objęci programem szkoleń w zakresie cyberbezpieczeństwa. Niezbędne jest więc przeszkolenie w powyższym zakresie zarówno kierownictwa i osoby odpowiedzialnej za bezpieczeństwo informacji, jak i wszystkich pracowników Urzędu pracujących z komputerami (W.07). W tym celu zakupiony zostanie 2 letni dostęp do profesjonalnej platformy elearningowej oferującej kompleksowe i cykliczne szkolenie w zakresie cyberbezpieczeństwa. Dla kadry kierowniczej przewidziano dodatkowe szkolenie stacjonarne w zakresie polityk oraz regulacji dotyczących bezpieczeństwa informacji (W.02, W.03, W.05, W.06, W.12, W.14), systemu zarządzania bezpieczeństwem informacji (W.24), a także zagadnień związanych identyfikacją i zarządzaniem ryzykiem (W.04) oraz incydentami (W.23, W.31, W.32, W.33). W związku z wdrażaniem w ramach projektu nowych technologii oraz systemów informatycznych, dla 4 pracowników IT przewidziano cykl szkoleń w zakresie bezpieczeństwa sieci, nowych systemów operacyjnych, systemów kopii bezpieczeństwa, oprogramowania antywirusowego z EDR oraz MDM, SIEM, SYSLOG, DLP, (W.07). Koszty usług szkoleniowych oszacowano na podstawie dostępnych na rynku ofert. Zadanie 3. Obszar techniczny. Realizacja zadania zaspokoi potrzeby UG Lesznowola w zakresie podniesienia poziomu cyberbezpieczeństwa infrastruktury IT Urzędu poprzez zakup specjalistycznego sprzętu oraz oprogramowania. Wzmocnienie cyberbezpieczeństwa jednostki realizowane będzie w obszarze ochrony sieci, ochrony danych i ich kopii zapasowych oraz ochrony na poziomie punktów końcowych. W zakresie wzmocnienia bezpieczeństwa sieci informatycznej Urzędu, w projekcie przewidziano wdrożenie kompleksowego systemu bezpieczeństwa sieci, składającego się z firewalla UTM nowej generacji oraz oprogramowania typu NAC. System taki będzie wspierał administratora w zarządzaniu siecią w zakresie: kontroli i zarządzania dostępem do sieci, nadawania uprawnień (W.06, W.08, W.14, W.17, W. 19), podglądu i monitorowania sieci i jej użytkowników (W.04, W.08, W. 09, W.10, W.12, W.14, W.16, W.17, W.19, W.25), zarządzaniu adresacją IP, a także w wykrywaniu zagrożeń i raportowaniu zdarzeń (W. 08, W.09, W.31). W zakresie ochrony danych i ich kopii zapasowych w projekcie przewidziano zakup i wdrożenie kompleksowego systemu bezpieczeństwa (W.17), składającego się z serwera, dwóch macierzy dyskowych oraz oprogramowania do zarządzania systemem. Serwer stanowił będzie platformę pod maszyny wirtualne obsługujące system archiwizacji danych. Serwer zostanie zakupiony wraz z systemem operacyjnym, środowiskiem do wirtualizacji Data Center oraz licencjami dostępowymi. Zakup nowego serwera umożliwi także efektywniejsze zarządzanie archiwizacją danych dzięki możliwości oddzielenia systemu kopii zapasowych od środowiska produkcyjnego. System uzupełniać będzie macierz dyskowa podstawowa oraz oddzielna macierz

	dedykowana do archiwizacji kopii zapasowych (W.16) oraz oprogramowanie umożliwiające scentralizowane zarządzanie archiwizacją i odzyskiwaniem danych, w tym na zautomatyzowane tworzenie kopii zapasowych, szybkie odzyskiwanie danych po awarii oraz pełną analitykę kopii zapasowych. Takie rozwiązanie umożliwiać będzie kompleksową ochronę danych (W.17), ochronę plików systemowych (W.19), bezpieczne przechowywanie zapisu dzienników systemowych (W.28), a także zabezpieczać będzie Urząd przed możliwością modyfikacji, usunięcia lub zniszczenia/utraty tych danych (W.12, W.16, W.17, W.19). W projekcie przewidziano zakup nowego centralnego UPS zdolnego podtrzymać pracę wszystkich zakupionych w projekcie urządzeń (W.16), ponieważ obecnie wykorzystywany nie spełnia wymagań jakościowych (8 lat użytkowania) oraz funkcjonalnych związanych z możliwością jego monitoringu i zarządzania. W zakresie ochrony urządzeń końcowych, w projekcie przewidziano odnowienie licencji na oprogramowanie antywirusowe oraz jej rozszerzenie o funkcjonalność EDR (W.09, W.10), a także wdrożenie oprogramowania klasy UEM do kompleksowego i zautomatyzowanego zarządzania aktywami IT, umożliwiającego m.in. inwentaryzację oraz audyt aktywów (W.03, W.15, W.16), skanowanie podatności oraz wykrywanie luk w zabezpieczeniach (W.04, W.09, W.10, W.15, W.19, W.20, W.21, W.22), zdalne zarządzanie konfiguracją urządzeń i oprogramowania, scentralizowaną dystrybucję oprogramowania systemowego, aktualizacji i poprawek (W.04, W.10, W.14, W.15, W.17, W.22), stałe monitorowanie i wykrywanie nieautoryzowanego sprzętu i oprogramowania w systemie (W.03, W.08, W.09, W.19) oraz scentralizowane zarządzanie uprawnieniami (W.06, W.08, W.10, W.11, W.17, W.19,). Koszty zakupu sprzętu i oprogramowania oszacowano na podstawie dostępnych na rynku ofert. Projekt na każdym etapie realizowany będzie zgodnie przepisami antydyskryminacyjnymi oraz zasadami równości szans ze względu na płeć, rasę, pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek oraz orientację seksualną. Rezultaty oraz produkty projektu będą powszechnie dostępne oraz nie będą dyskryminacyjne. Wnioskodawca zapewni zgodność projektu z zasadami równości szans kobiet i mężczyzn oraz dostępności dla osób z niepełnosprawnościami. W projekcie obowiązywać będą standardy dostępności, w tym standardy dostępności cyfrowej. Stworzone w projekcie zasoby cyfrowe, np. strona www będą zgodne ze standardem WCAG 2.1. W projekcie nie występują bariery równościowe w obszarze zakresu ani zasięgu jego oddziaływania. Projekt będzie miał pozytywny wpływ na politykę równych szans i niedyskryminacji. W obszarze technicznym i organizacyjnym dotyczącym zakupu sprzętu informatycznego, oprogramowania oraz usług doradczych Wnioskodawca zapewni zgodność projektu z zasadą równości szans poprzez zastosowanie deklaracji przestrzegania zasad równościowych przez wykonawców na etapie procedury zakupowej. W obszarze kompetencyjnym Wnioskodawca zapewni spełnienie zasad dostępności oraz wymagań równościowych i antydyskryminacyjnych poprzez organizację szkoleń w sposób zapewniający równy dostęp dla wszystkich pracowników, w tym osób z niepełnosprawnościami. Treść szkoleń musi być zrozumiała dla każdego uczestnika bez względu na jego doświadczenie, wiedzę, umiejętności językowe, a także dostosowana do potrzeb osób z niepełnosprawnościami. Równość szans kobiet i mężczyzn zapewni indywidualnie określany przez uczestników harmonogram szkolenia, dostosowany do ich indywidualnej organizacji czasu pracy, w tym konieczności wypełniania obowiązków rodzinnych.
Projekt grantowy	Tak

2. Miejsce realizacji projektu

Obszar realizacji projektu (TERYT)	1418032
Maksymalna kwota dofinansowania grantu dla Beneficjenta (liczona po współczynniku dochodów Beneficjenta (w PLN)	850000,00
Minimalna wysokość wkładu własnego (wyrażona w %)	20,00
Procent dofinansowania UE (w %)	72,80
Procent dofinansowania BP (w %)	7,20
Województwo/Powiat/Gmina	MAZOWIECKIE/piaseczyński/Lesznowola

3. Informacje o Grantobiorcy

NIP	1231220334
Nazwa Grantobiorcy	GMINA LESZNOWOLA
Regon	013271111
KRS	*brak danych*
Forma Prawna Grantobiorcy	WSPÓLNOTY SAMORZĄDOWE
Możliwość odzyskania VAT	Tak

Adres siedziby

Kraj	Polska
Miejscowość	Lesznowola
Kod pocztowy	05-506
Ulica	ul. Gminna
Nr domu	60
Nr lokalu (opcjonalnie)	*nie dotyczy*
Adres e-mail	gmina@lesznowola.pl
Adres ePUAP	/apq4u8b94x/SkrytkaESP
Nr tel	+48 227089111

Adres korespondencyjny

Adres korespondencyjny taki sam jak adres firmy	tak

Osoba upoważniona do kontaktu

Imię	Joanna
Nazwisko	Misiak
Stanowisko	Gł. specjalista
Adres e-mail	rfz@lesznowola.pl

Nr tel	+48 227089131
Nr rachunku bankowego Grantobiorcy	38 9288 0001 5500 0257 2000 0280

Osoby upoważnione do reprezentacji Grantobiorcy

Imię	Maria Jolanta
Nazwisko	Batycka-Wąsik
Stanowisko	Wójt Gminy Lesznowola
Podpis/kontrasygnata	podpis
Adres e-mail	wojt@lesznowola.pl
Nr tel	+48 227089111

Imię	Marta Magdalena
Nazwisko	Sulimowicz
Stanowisko	Skarbnik Gminy
Podpis/kontrasygnata	kontrasygnata
Adres e-mail	marta.sulimowicz@lesznowola.pl
Nr tel	+48 227089217

4. Zakres rzeczowy projektu

Zadanie

Nazwa zadania	Obszar organizacyjny

Zadanie

Nazwa zadania	Obszar kompetencyjny

Zadanie

Nazwa zadania	Obszar techniczny

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	Testy podatności - usługa doradcza specjalistyczna	8 000,00	1	8 000,00	8 000,00	0,00	6 400,00	1 600,00

2	Audyt zgodności z KRI UoKSC - usługa doradcza specjalistyczna	9 000,00	1	9 000,00	9 000,00	0,00	7 200,00	1 800,00
3	Aktualizacja PBI oraz analiza ryzyka w tym opracowanie i wdrożenie metodyk - usługa doradcza specjalistyczna	14 000,00	1	14 000,00	14 000,00	0,00	11 200,00	2 800,00
4	Aktualizacja SZBI - usługa doradcza specjalistyczna	14 000,00	1	14 000,00	14 000,00	0,00	11 200,00	2 800,00
5	Audyt końcowy - usługa doradcza specjalistyczna	12 000,00	1	12 000,00	12 000,00	0,00	9 600,00	2 400,00
6	Promocja - usługa zlecona	2 000,00	1	2 000,00	2 000,00	0,00	1 600,00	400,00
			SUMA	59 000,00	59 000,00	0,00	47 200,00	11 800,00

Zadanie 2 - 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	Szkolenie z podstaw cyberbezpieczeństwa dla pracowników - platforma e-learningowa 2 lata - usługa zlecona	90,00	150	13 500,00	13 500,00	0,00	10 800,00	2 700,00
2	Szkolenie IT - Bezpieczeństwo sieci komputerowych testy penetracyjne - usługa zlecona	4 400,00	4	17 600,00	17 600,00	0,00	14 080,00	3 520,00

3	Szkolenie stacjonarne dla kadry kierowniczej - usługa zlecona	3 900,00	1	3 900,00	3 900,00	0,00	3 120,00	780,00
4	Szkolenie IT - Fortigate - usługa zlecona	2 000,00	4	8 000,00	8 000,00	0,00	6 400,00	1 600,00
5	Szkolenie IT - system kopii bezpieczeństwa - usługa zlecona	2 300,00	4	9 200,00	9 200,00	0,00	7 360,00	1 840,00
6	Szkolenie IT - zarządzenie w IT - usługa zlecona	13 000,00	4	52 000,00	52 000,00	0,00	41 600,00	10 400,00
7	Szkolenie IT - Bezpieczeństwo Windows - usługa zlecona	3 000,00	4	12 000,00	12 000,00	0,00	9 600,00	2 400,00
8	Szkolenie IT - MS 55345 Zarządzanie i wdrażanie Windows 11 - usługa zlecona	3 700,00	4	14 800,00	14 800,00	0,00	11 840,00	2 960,00
			SUMA	131 000,00	131 000,00	0,00	104 800,00	26 200,00

Zadanie 3 - 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	Serwer	90 000,00	1	90 000,00	90 000,00	0,00	72 000,00	18 000,00
2	Macierz do systemów wdrażanych w ramach projektu	115 000,00	1	115 000,00	115 000,00	0,00	92 000,00	23 000,00
3	Macierz do kopii zapasowych	110 000,00	1	110 000,00	110 000,00	0,00	88 000,00	22 000,00
4	Oprogramowanie do kopii zapasowych	70 000,00	1	70 000,00	70 000,00	0,00	56 000,00	14 000,00
5	Firewall sieciowy	50 000,00	1	50 000,00	50 000,00	0,00	40 000,00	10 000,00

6	Licencja na oprogramowanie Network Access Control NAC	80 000,00	1	80 000,00	80 000,00	0,00	64 000,00	16 000,00
7	UPS centralny	80 000,00	1	80 000,00	80 000,00	0,00	64 000,00	16 000,00
8	Licencja oprogramowania antywirus z modułem EDR dla stanowisk	35 000,00	1	35 000,00	35 000,00	0,00	28 000,00	7 000,00
9	Licencja na oprogramowanie: MDM, SIEM, SYSLOG, DLP	150 000,00	1	150 000,00	150 000,00	0,00	120 000,00	30 000,00
10	Switch zarządzany	10 000,00	3	30 000,00	30 000,00	0,00	24 000,00	6 000,00
			SUMA	810 000,00	810 000,00	0,00	648 000,00	162 000,00

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	1 000 000,00	1 000 000,00	0,00	800 000,00	200 000,00

Podsumowanie budżetu

	Wydatki ogółem (w PLN)	Wydatki kwalifikowalne (w PLN)	Dofinansowanie (w PLN)
Razem w projekcie	1 000 000,00	1 000 000,00	800 000,00

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
1 000 000,00	1 000 000,00	800 000,00	80,00	728 000,00	72,80	7,20	72 000,00	200 000,00	200 000,00	20,00

7. Źródła finansowania wydatków (w PLN)

	Wydatki ogółem	Wydatki kwalifikowalne
Dofinansowanie	800 000,00	800 000,00

Razem wkład własny:	200 000,00	200 000,00
Budżet państwa	0,00	0,00
Budżet Jednostek Samorządu Terytorialnego	200 000,00	200 000,00
Inne publiczne	0,00	0,00
Prywatne	0,00	0,00
SUMA	1 000 000,00	1 000 000,00

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).	☑
Oświadczam, że zapoznałem się/zapoznałam się z Regulaminem naboru i akceptuję jego zasady.	☑
Oświadczam, że nie podlegam wykluczeniu z możliwości otrzymania dofinansowania ze środków UE.	☑
Oświadczam, że podane przeze mnie dane w Formularzu Aplikacyjnym o grant i złożone oświadczenia są prawdziwe.	☑
Zobowiązuję się, w przypadku pozytywnego rozpatrzenia mojego wniosku, do przesłania dokumentów potwierdzających upoważnienie do reprezentacji dla osób podpisujących umowę grantową.	☑
Oświadczam, że zapoznałem/am się i akceptuję warunki Kompletnego Schematu Grantowego w projekcie "Cyberbezpieczny Samorząd" i zobowiązuję się do jego przestrzegania.	☑
Oświadczam, że przestrzegam przepisów dotyczących zasad horyzontalnych, o których mowa w art. 9 lub motywie 6 rozporządzenia nr 2021 /1060.	☑
Oświadczam, że w związku z aplikowaniem w projekcie „Cyberbezpieczny Samorząd" nie jestem podatnikiem VAT i w okresie realizacji projektu FERC nie będzie podejmowana działalność, której skutkiem będzie nabycie statusu podatnika VAT albo jestem podatnikiem VAT zarejestrowanym we właściwym dla siebie urzędzie skarbowym, który w okresie realizacji projektu w zakresie nabyć objętych wnioskiem o dofinansowanie projektu FERC nie będzie miał prawnej możliwości odzyskania VAT.	☐
Oświadczam, że nie podlegam pomocy publicznej nie otrzymałem/łam pomocy de minimis na przedsięwzięcie, na którego realizację złożony został wniosek o dofinansowanie.	☑

Załączniki

Dokumenty potwierdzające prawo do reprezentacji Grantobiorcy

Nazwa	Rozmiar	Suma kontrolna
Zaświadczenie o wyborze Wójta Lesznowola-sig-sig.pdf	465 KB	2c7198fa6ab4d2e02e175b31f7b0ae6c302723a8bf575544c064796c85c4e517
Powołanie Skarbnika Lesznowola-sig-sig.pdf	454 KB	6666fee6d5297c2b03eb37ab46ef515904a1b5f9f58a56868e662a52d5b4365b

Oświadczenie Grantobiorcy dot. VAT

Nazwa	Rozmiar	Suma kontrolna
Oświadczenie dot kwalifikowalności podatku VAT puste-sig-sig.pdf	1 MB	75321340aeac51e887789244e1d0c45be9722b329a7cc515a5c75b76db9d8b65

Dodatkowe dokumenty ze strony Grantobiorcy

Nazwa	Rozmiar	Suma kontrolna
brak załączników		