Urząd Miejski w Brzostku

woj. podkarpackie

ul. Rynek 1, 39-230 Brzostek

tel: 146803026, e-mail: sekretariat@brzostek.pl, Nip: 872-11-99-898, Regon: 000533239

[redacted]

SO.1431.30.2025

Brzostek, 8 kwietnia 2025 r.

Burmistrz Brzostku w odpowiedzi na wniosek o udostępnienie informacji publicznej z dnia 26.03.2025 r. dot. realizacji projektu „Cyberbezpieczny Samorząd" w Gminie Brzostek w załączeniu przekazuje odpowiedź w formacie pliku pdf zgodnie z Pana żądaniem.

BURMISTRZ

mgr inż. Zbigniew Kowalski

Załączniki:

1. Wniosek (format pdf)
2. Załączniki do wniosku

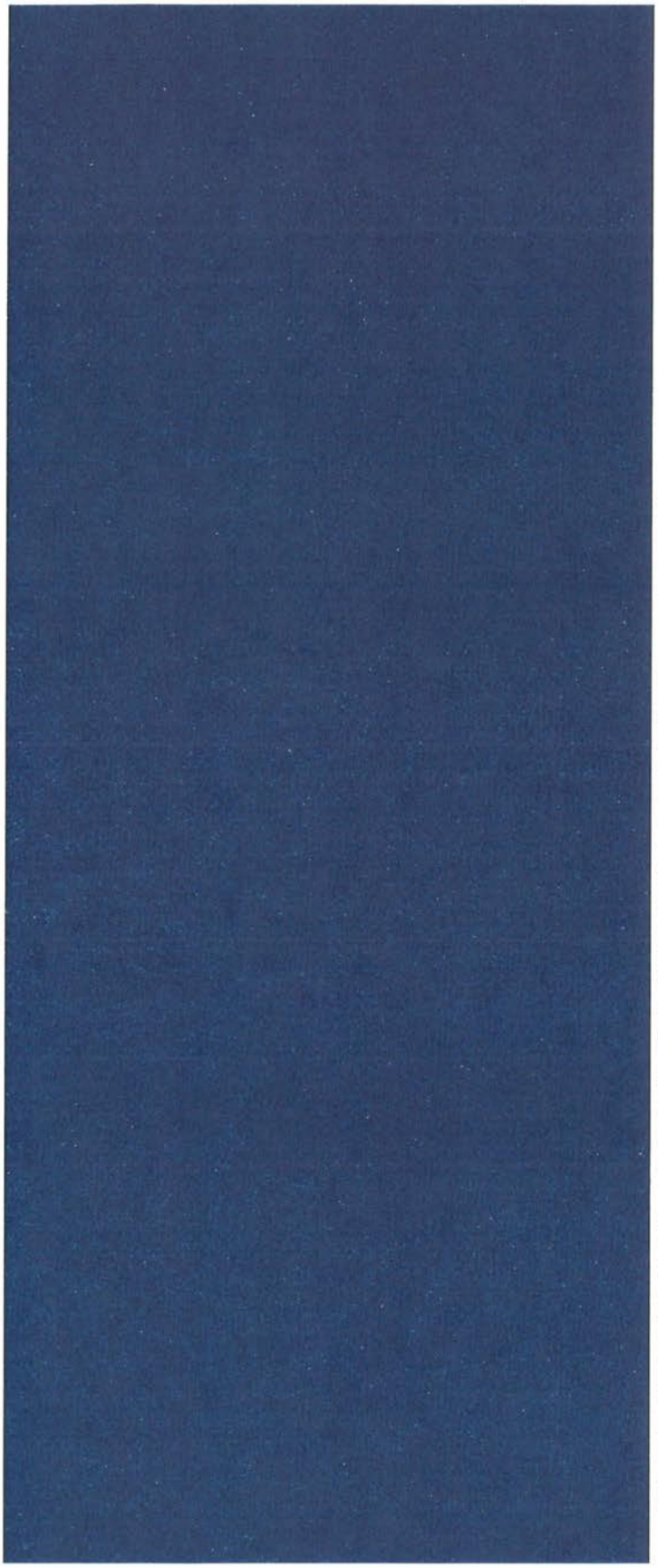
Systemowy identyfikator wniosku	dc189ac4-e08b-4475-b02d-de831f8c4755

1. Informacje ogólne o projekcie

Data złożenia wniosku	2023-12-07 08:30:37
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	Wzmocnienie cyberbezpieczeństwa w Urzędzie Miejskim w Brzostku
	Celem projektu jest zwiększenie bezpieczeństwa informacji w Urzędzie Miejskim w Brzostku poprzez wzmocnienie jej odporności i zdolności do zapobiegania, wykrywania oraz reagowania na incydenty bezpieczeństwa teleinformatycznego. Projekt obejmuje opracowanie dokumentacji SZBI, szkolenia pracowników, zakup, wdrożenie i utrzymanie urządzeń i oprogramowania, zapewnienie ciągłości pracy urzędu przez zakup agregatu prądotwórczego. Jest zgodne z celem szczegółowym Działania FERC.02.02 - Wzmocnienie krajowego systemu cyberbezpieczeństwa, mającego na celu czerpanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych. Powyższy projekt został zaplanowany z neutralnością dla zasady równości kobiet i mężczyzn. Planowane działania zostały dostosowane tak, że wykazują one równe szanse korzystania z efektów projektu każdej płci. Podejście Wnioskodawcy, jest pełne zrozumienia dla potrzeb osób z niepełnosprawnościami, co oznacza, że infrastruktura i materiały projektowe spełniają standardy dostępności cyfrowej, aby umożliwić dostępność naszych działań dla wszystkich. Projekt jest zgodny z obowiązującymi standardami dostępności dla polityk spójności i jest neutralny wobec zasady równości kobiet i mężczyzn, z uwzględnieniem możliwości dostosowywania działań w odpowiedzi na diagnozowane nierówności. I)Obszar techniczny. Brak oprogramowania i usług przed reakcją na zagrożenia cyberataku. 1)(W16)Zabezpieczenie poczty elektronicznej w Urzędzie poprzez zakup lokalnego serwera pocztowego głównego i zapasowego o takiej samej konfiguracji dla utrzymania ciągłości pracy usł. pocztowej oraz redundancji. Zabezpieczenie poczty polegać będzie na integracji serwerów poczty lokalnej z serwerem hostingowym tak aby emaile i dokumenty przechowywane oraz archiwizowane były wewnątrz Urzędu oraz dodatkowo sprawdzane przez antywirusa, antyspama, reguły DLP. Serwer poczty lokalnej zapewni monitoring i wyświetlenie komunikatu dla użytkownika o wycieku adresów email podczas wysłania wiadomości email. Serwery lokalne poczty muszą być zintegrowane z kontrolerem domeny, a każda zmiana hasła użytkownika również zostanie uwzględniona dla konta email. Użytkownicy na komputerach lokalnych będą mogli uruchamiać podejrzane pliki i załączniki poczty w środowisku sandbox. Rozszerzenie posiadanego oprogramowania RODOCrypt o dodatkowe moduły z bezpieczeństwa teleinformatycznego: RODOCrypt_Sandbox: możliwość uruchomienia plików, załączników oraz wiadomości e-mail w testowym i odseparowanym od systemu użytkownika środowisku sandbox. Takie odseparowanie środowisk pozwoli zabezpieczyć komputery przed infekcją wirusów, koni trojańskich, a także ransomware. Podejrzane email i załączniki mogą być

Koncepcja realizacji

wysyłane do administratora w celu sprawdzenia ich w odseparowanym środowisku sandbox.
RODOCrypt_EmailLeak: moduł integrujący się z klientami MS Outlook i Thunderbird zapewni monitoring i wyświetlenie komunikatu dla użytkownika o wycieku adresów email wraz z decyzją czy dany email będzie szyfrowany technologią END TO END podczas wysłania wiadomości.
2)(W19)Macierze dyskowe nie są jedynie sprzętem, przede wszystkim to dedykowane oprogramowania, pozwalające na zarządzanie zasobami, ich podziałem, kopiami bezpieczeństwa, klonowaniem oraz replikacją. Zakup dwóch macierzy pozwoli synchronizować dane pomiędzy urządzeniami zlokalizowanymi w dwóch oddzielnych od siebie pomieszczeniach (serwerowniach) zlokalizowanych w budynku Urzędu Miejskiego w Brzostku.
3)(W10)Zakup brzegowych Firewall'i do zabezpieczania sieci lokalnej oraz styku z Internetem. Urządzenia FortiGate łączą w sobie funkcje antywirusowe, pracują jako filtr spamu, stron WWW, umożliwiają zarządzanie pasmem (Qos) oraz mają wpływ na kontrolę komunikatorów sieciowych i aplikacji P2P. Zastosowanie dwóch urządzeń pozwoli dokładniej zabezpieczyć sieć, rozdzielić zadania. Ponadto poczta email pracowników urzędu będzie sprawdzana pod kątem ewentualnej obecności wirusów, trojanów oraz spamu. Urządzenia FortiGate oferują kilka poziomów ochrony zaczynając od filtrowania stron WWW i blokowania phishingu, kończąc na zapobieganiu włamaniom i próbom przejęcia kontroli nad przeglądarkami. Rozwiązania te swoją skuteczność osiągają dzięki wykorzystaniu kombinacji dwóch mechanizmów ochronnych: analizy heurystycznej oraz metod sygnałowych, co umożliwia efektywne zatrzymanie szkodników każdego typu. Malware, oprogramowanie szpiegowskie, keyloggery, ransomware to przykładowe zagrożenia, które FortiGate namierzy i powstrzyma. Zintegrowane technologie bezpieczeństwa pozwalają sprawnie chronić zarówno pracowników na miejscu, w firmie, jak i w terenie (mobilnych). Opcja nawiązywania połączeń poprzez VPN daje możliwość przesyłania danych bez ryzyka, że ktokolwiek będzie w stanie je przejąć.
4)(W09)Urządzenie służące do zapisywania zdarzeń oraz raportowania. Jego zadaniem jest zbieranie, a następnie przetwarzanie danych ze wszystkich urządzeń i narzędzi zainstalowanych w sieci lokalnej urzędu. FortiAnalyzer, to rozwiązanie, które bezpiecznie zbiera i analizuje dane przekazywane z różnych urządzeń Fortinet oraz innych narzędzi kompatybilnych z serwerem SYSLOG. System dostarcza administratorom sieci wyczerpujący obraz wykorzystania sieci i bezpieczeństwa informacji w całym przedsiębiorstwie, co minimalizuje wysiłek związany z monitorowaniem i utrzymaniem polityki wykorzystania zasobów, identyfikacją ataków, wyciągania konsekwencji wobec atakujących i przestrzeganiem przepisów prawa dotyczących prywatności i bezpieczeństwa poufnych danych. Urządzenia FortiAnalyzer pobierają i przetwarzają pełny zakres informacji dotyczących ruchu, zdarzeń, wirusów, ataków, filtrowania treści www i e-mail oraz realizują zaawansowane funkcje zarządzania bezpieczeństwem, takie jak archiwizacja informacji o kwarantannach, korelacja zdarzeń, ocena podatności na zagrożenia, analiza ruchu, archiwizacja treści. Urządzenie pozwala na tworzenie szerokiego zakresu raportów, które w czytelny sposób obrazują pracę naszej sieci.
5)(W10)Jest to rozwiązanie zapewniające ochronę punktom końcowym oraz innowacyjny rodzaj zabezpieczenia przed wszelkimi zagrożeniami. Ochrona punktów końcowych jest szczególnie ważnym zagadnieniem dla klientów końcowych, ponieważ to właśnie oni są najbardziej narażeni na wszelkie ataki oraz zarażenie złośliwym oprogramowaniem. FortiClient doceniany jest głównie ze względu na możliwość tworzenia



połączeń wirtualnej sieci prywatnej nazywanej w skrócie VPN. Jest to rodzaj platformy, która służy przede wszystkim do zabezpieczania końcowych stacji. To właśnie one stanowią jeden z częstszych celów wielu ataków hackerskich.
6)(W19)Karta SFP służy do bezpiecznego połączenia sieci internetowej z siecią lokalna. korzystanie z modułu światłowodowego SFP jest bezpieczniejsze niż kabla Ethernet. Kabel RJ45 wykorzystuje prąd elektryczny, dzięki czemu łatwiej jest zapalić się od ognia/pioruna, podczas gdy moduł światłowodowy SFP nie ma takiego problemu. Niezawodność. Włókno jest często uważane za bardziej niezawodne ze względu na swoje właściwości.
7,8) Planowany zakup to urządzenia w postaci switchy zarządzanych. Modele zarządzalne to idealny sposób na ochronę najważniejszych danych poprzez system IP Security lub filtrowanie bezpiecznych adresów MAC. W ten sposób mamy pewność, że wszystkie nasze hasła nie wpadną w niepowołane ręce.
9)(W19)VMware - Umożliwia uruchamianie w jednym systemie macierzystym wielu wirtualnych maszyn do różnych celów. VMware to jedno z najpopularniejszych oprogramowań do wirtualizacji. Pozwala na łatwe zarządzanie infrastrukturą IT. Dzięki wykorzystaniu jednego narzędzia, wydajność oraz elastyczność zasobów rośnie, jest jednym z najbezpieczniejszych hypervisorów w branży IT. Program ten został obdarzony wysokim zaufaniem ze względu na bezpieczeństwo sieci.
10) (W03)Montaż, instalacja oraz konfiguracją sprzętu i oprogramowania.
11) (W03)Antywirus - to specjalistyczne oprogramowanie zaprojektowane do wykrywania, neutralizowania i usuwania wszelkiego rodzaju złośliwego oprogramowania czyli malware. Malware obejmuje wiele różnych form szkodliwego oprogramowania, takich jak wirusy, trojany, robaki, spyware, adware, ransomware.
12) (W19)Baterie - wymiana w celu podtrzymania energii dla serwerów.
13) (W16)Serwer - Wymiana serwera na nowy wraz z oprogramowaniem zapewni bezpieczeństwo danych oraz usprawni pracę.
14) (W19)Zakup agregatu prądotwórczego z osprzętem - urząd boryka się z częstymi przerwami w zasilaniu, dlatego zakup agregatu prądotwórczego o mocy min. 60 kW. Brak magazynu energii i krótki czas podtrzymania przez zasilacze awaryjne naraża systemy IT na ryzyko utraty danych i uszkodzeń. Nowy agregat zapewni ochronę przed awariami związanymi z przerwami w dostawach energii elektrycznej, zabezpieczając systemy IT w każdym obszarze.
II)(W01)Obszar organizacyjny - brak obowiązującego SZBI w UM
Uzasadnienie: SZBI to strategia działania, której celem jest zapewnianie właściwej ochrony informacji. Strategia ta ma zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyk związanych z naruszeniem poufności. Prawidłowo przygotowany i wdrożony SZBI chroni poufne informacje (w tym również dane osobowe) przed kradzieżą, zgubieniem, nieuprawnionym wykorzystaniem, a także przed celowym lub przypadkowym usunięciem. Opracowanie oraz wdrożenie w UM w Brzostku dokumentacji SZBI uchroni pracowników oraz interesantów przed utratą danych, wprowadzi standardy oraz wpłynie na podniesienie poziomu bezpieczeństwa.
III)(W07)Obszar kompetencyjny - niewystarczająca wiedza pracowników dot. obsługi sprzętu i oprogramowania.
Uzasadnienie: Ważną kwestią przy wdrażaniu nowych rozwiązań, aby w pełni wykorzystać możliwości sprzętowe i programistyczne jest organizacja szkoleń dla pracowników. Zminimalizowanie liczby występowania incydentów poprzez umiejętną edukację pracowników.

	Podniesienie świadomości na temat cyberzagrożeń w organizacji. Poznanie tech. podstaw cyberbezpiecze. dot. ochrony danych.
Projekt grantowy	Tak

2. Miejsce realizacji projektu

Obszar realizacji projektu (TERYT)	1803023
Maksymalna kwota dofinansowania grantu dla Beneficjenta (liczona po współczynniku dochodów Beneficjenta (w PLN)	850000,00
Minimalna wysokość wkładu własnego (wyrażona w %)	0,00
Procent dofinansowania UE (w %)	81,00
Procent dofinansowania BP (w %)	19,00
Województwo/Powiat/Gmina	PODKARPACKIE/dębicki/Brzostek

3. Informacje o Grantobiorcy

NIP	8722223191
Nazwa Grantobiorcy	GMINA BRZOSTEK
Regon	851661085
KRS	*brak danych*
Forma Prawna Grantobiorcy	WSPÓLNOTY SAMORZĄDOWE
Możliwość odzyskania VAT	Nie

Adres siedziby

Kraj	Polska
Miejscowość	Brzostek
Kod pocztowy	39-230
Ulica	ul. Rynek
Nr domu	1
Nr lokalu (opcjonalnie)	*nie dotyczy*
Adres e-mail	sekretariat@brzostek.pl
Adres ePUAP	/5qkbn721sf/SkrytkaESP
Nr tel	+48 146803026

Adres korespondencyjny

Adres korespondencyjny taki sam jak adres firmy	tak

Osoba upoważniona do kontaktu

Imię	Grzegorz
Nazwisko	Kudłacz

Stanowisko	Informatyk
Adres e-mail	Informatyk@brzostek.pl
Nr tel	+48 146803018
Nr rachunku bankowego Grantobiorcy	48 8589 0006 0080 0210 2020 0203

Osoby upoważnione do reprezentacji Grantobiorcy

Imię	Wojciech
Nazwisko	Staniszewski
Stanowisko	Burmistrz
Podpis/kontrasygnata	podpis
Adres e-mail	burmistrz@brzostek.pl
Nr tel	

Imię	Elżbieta
Nazwisko	Łukasik
Stanowisko	Skarbnik
Podpis/kontrasygnata	kontrasygnata
Adres e-mail	skarbnik@brzostek.pl
Nr tel	+48 146803017

4. Zakres rzeczowy projektu

Zadanie

Nazwa zadania	Obszar techniczny

Zadanie

Nazwa zadania	Obszar organizacyjny

Zadanie

Nazwa zadania	Obszar kompetencyjny

5. Zakres finansowy

Wydatki rzeczywiście ponoszone

Zadanie 1 - 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 pocztowy - podstawowy i zapasowy	200 000,00	1	200 000,00	200 000,00	0,00	200 000,00	0,00
2	Zakup macierzy dyskowej	101 000,00	2	202 000,00	202 000,00	0,00	202 000,00	0,00
3	Zakup UTM	25 000,00	2	50 000,00	50 000,00	0,00	50 000,00	0,00
4	FortiAnalyzer	28 290,00	1	28 290,00	28 290,00	0,00	28 290,00	0,00
5	FortiClient	8 610,00	1	8 610,00	8 610,00	0,00	8 610,00	0,00
6	Karta SFP	1 845,00	2	3 690,00	3 690,00	0,00	3 690,00	0,00
7	SWITCH szkieletowy	2 952,00	2	5 904,00	5 904,00	0,00	5 904,00	0,00
8	SWITCH dostępowy	4 428,00	2	8 856,00	8 856,00	0,00	8 856,00	0,00
9	VMware	33 210,00	1	33 210,00	33 210,00	0,00	33 210,00	0,00
10	Prace konfiguracyjne wraz z materiałami montażowymi, kable połączeniowe	20 000,00	1	20 000,00	20 000,00	0,00	20 000,00	0,00
11	Antywirus dla 15 użytkowników	322,00	15	4 830,00	4 830,00	0,00	4 830,00	0,00
12	Wymiana bateri w istniejącym UPS-e	2 000,00	1	2 000,00	2 000,00	0,00	2 000,00	0,00
13	Serwer wraz z oprogramowaniem	67 610,00	1	67 610,00	67 610,00	0,00	67 610,00	0,00
14	Agregat prądotwórczy z osprzętem	100 000,00	1	100 000,00	100 000,00	0,00	100 000,00	0,00
			SUMA	735 000,00	735 000,00	0,00	735 000,00	0,00

Zadanie 2 - 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	Opracowanie dokumentacji SZBI	55 000,00	1	55 000,00	55 000,00	0,00	55 000,00	0,00
			SUMA	55 000,00	55 000,00	0,00	55 000,00	0,00

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	Szkolenie dla informatyka w zakresie konfiguracji infrastruktury i jej zarządzania konfiguracja domeny, zarządzania AD, UTM	20 000,00	1	20 000,00	20 000,00	0,00	20 000,00	0,00
2	Szkolenie dla kadry zarządzającej oraz pracowników w zakresie zastosowanych środków bezpieczeństwa oraz cyberbezpieczeństwa w ramach projektu grantowego	500,00	40	20 000,00	20 000,00	0,00	20 000,00	0,00
3	Doradztwo w zakresie bezpieczeństwa	20 000,00	1	20 000,00	20 000,00	0,00	20 000,00	0,00
			SUMA	60 000,00	60 000,00	0,00	60 000,00	0,00

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	850 000,00	850 000,00	0,00	850 000,00	0,00

Podsumowanie budżetu

	Wydatki ogółem (w PLN)	Wydatki kwalifikowalne (w PLN)	Dofinansowanie (w PLN)
Razem w projekcie	850 000,00	850 000,00	850 000,00

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

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
zaswiadczenie burmistrz.pdf	270 KB	879efa4e6d70f52eb3c71a388712afa1757c9a07237a608df09914644fc0ddef
powołanie skarbnika.pdf	314 KB	23d1d9f58dbca58b8fb2581bfc374a50235f111fdf90a608e93fbfa956c93e25

Oświadczenie Grantobiorcy dot. VAT

Nazwa	Rozmiar	Suma kontrolna
Załącznik_nr_7_-_Oświadczenie_dotyczące_kwalifikowalności_podatku_VAT.pdf	735 KB	b1cf40ee6c594a303ecaafb6c80e42065925dcd71dd463f9c71cd294cfd80c83

Dodatkowe dokumenty ze strony Grantobiorcy

Nazwa	Rozmiar	Suma kontrolna
brak załączników		

850 000,00	850 000,00	850 000,00	100,00	688 500,00	81,00	19,00	161 500,00	0,00	0,00	0,00

7. Źródła finansowania wydatków (w PLN)

	Wydatki ogółem	Wydatki kwalifikowalne
Dofinansowanie	850 000,00	850 000,00
Razem wkład własny:	0,00	0,00
Budżet państwa	0,00	0,00
Budżet Jednostek Samorządu Terytorialnego	0,00	0,00
Inne publiczne	0,00	0,00
Prywatne	0,00	0,00
SUMA	850 000,00	850 000,00

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.	☑