WNIOSKODAWCA:
Nazwisko i Imię: Jan Świeży

GMINA ZŁOTA
ul. Sienkiewicza 79
28-425 Złota

WNIOSEK
O UDOSTĘPNIENIE INFORMACJI PUBLICZNEJ

Na podstawie art. 2 ust. 1 ustawy o dostępie do informacji publicznej z dnia 6 września 2001 roku (Dz. U. Nr 112, poz. 1198 z późn. zm.), zwracam się z prośbą o udostępnienie informacji w następującym zakresie:

Wniosek o udzielenie grantu w programie Cyberbezpieczny Samorząd o numerze FERC.02.02-CS.01-001/23/0617

SPOSÓB I FORMA UDOSTĘPNIENIA INFORMACJI:

proszę o przesłanie wniosku w formacie .pdf wraz z załącznikami pocztą elektroniczną na adres: informacja@cyberbezpiecznysamorzad.online

Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z ustawą z dnia 29.08.1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r. Dz. U. Nr 101, poz. 926 z późn. .zm.).

Katowice, 25.03.2024
Miejscowość, data

Jan Świeży
podpis wnioskodawcy

ug@gminazlota.pl

Od: ug@gminazlota.pl
Wysłano: środa, 2 kwietnia 2025 13:23
Do: 'informacja@cyberbezpiecznysamorzad.online'
Temat: Odpowiedź na wniosek o udostępnienie informacji publicznej
Załączniki: 0705_001.pdf

Dzień dobry,
W załączeniu odpowiedź na wniosek o udostępnienie informacji publicznej w formacie pdf. Proszę o potwierdzenie otrzymania wiadomości.

Urząd Gminy Złota
Sekretariat: Justyna Bąba
Tel. 41 356 16 01

Systemowy identyfikator wniosku	ee4c93aa-44ca-4973-a6c1-e042c88df453

1. Informacje ogólne o projekcie

Data złożenia wniosku	2023-12-06 13:29:09
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 Gminy Złota
	Celem projektu jest wzmocnienie cyberbezpieczeństwa w Urzędzie Gminy Złota. Jest to cel zgodny z celem szczegółowym Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa - czerpanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych, jak też z zapisem w Szczegółowym Opisie Priorytetów Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, wg którego projekty realizowane w ramach ww. działania "zapewnią sprawne i bezpieczne działanie systemów informatycznych oraz lepszą ochronę informacji". Efektem projektu będzie: 1) zakup i wdrożenie szeregu systemów i urządzeń podnoszących bezpieczeństwo informacji w urzędzie, takich jak: - urządzenie UTM wraz z licencjami na 24 miesiące;; - 3 switche zarządzalne, z możliwością integracji z urządzeniami UTM; - system do zbierania i analizy logów dedykowany dla zakupywanych urządzeń UTM, switchów i access pointów; - zasilacz awaryjny (UPS) 3kVA; - oprogramowanie antywirusowe - pakiet 45 licencji na 2 lata; - nowy serwer z systemem operacyjnym Windows Server i licencjami dostępowymi; - dedykowane urządzenie - serwer plików (Network Attached Storage - NAS) do bezpiecznego przechowywania danych. 2) wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji dostosowanego do potrzeb i warunków pracy urzędu, zgodnego z aktualnie obowiązującymi normami, w tym opracowanie dokumentacji zawierającej jego polityki i procedury, z uwzględnieniem technologii nowo zakupionych w ramach grantu, z doradztwem w zakresie diagnozy dojrzałości cyberbezpieczeństwa oraz audytem końcowym; 3) przeszkolenie pracowników urzędu (45 osób) w zakresie cyberbezpieczeństwa przy pomocy udostępnionej na 6 miesięcy platformy szkoleniowej; 4) przeszkolenie personelu IT w zakresie obsługi nowo zakupywanego NAS oraz w zakresie konfiguracji i zarządzania Active Directory pod kątem cyberbezpieczeństwa. Projekt będzie realizowany zgodnie z zasadami niedyskryminacji, dostępności dla osób niepełnosprawnościami oraz równości kobiet i mężczyzn. Dostawcy usług, szkoleń, oprogramowania i sprzętu będą wybierani zgodnie z tymi zasadami. W przetargach premiowani będą dostawcy prowadzący aktywną politykę niedyskryminacji (np. zatrudniający osoby z niepełnosprawnościami). Szkolenia, usługi i inne bezpośrednie prace (np. wdrażanie systemów) będą mogły świadczyć

[redacted]	osoby kompetentne bez względu na ich ewentualną niepełnosprawność czy płeć. Z uwagi na możliwość udziału w szkoleniach pracowników niepełnosprawnych będą one realizowane w miejscach bez barier dostępu lub zdalnie. Projekt zakłada zakup sprzętu informatycznego i oprogramowania, i w tym zakresie jest neutralny z punktu widzenia zasad niedyskryminacji oraz równości kobiet i mężczyzn. Zakupywane systemy będą dostępne dla osób z niepełnosprawnościami - urząd zgodnie z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności musi spełniać w swoich systemach teleinformatycznych co najmniej standard WCAG 2.0 i będzie go spełniać. UZASADNIENIE ZAKRESU WYDATKÓW: Zadanie: Poprawa bezpieczeństwa - obszar organizacyjny. W01 - W chwili obecnej w urzędzie nie ma wdrożonego kompletnego i zgodnego z aktualnymi normami Systemu Zarządzania Bezpieczeństwem Informacji. W celu zmiany tej sytuacji wnioskodawca planuje zakup usługi opracowania dokumentacji SZBI oraz wdrożenia SZBI, z uwzględnieniem nowych, zakupywanych w ramach grantu technologii, wraz z doradztwem w zakresie diagnozy dojrzałości cyberbezpieczeństwa oraz audytem końcowym. Zadanie: Poprawa bezpieczeństwa - obszar techniczny. W08, W09 - W chwili obecnej wnioskodawca nie dysponuje systemem monitorowania zdarzeń, który będzie analizował aktywność w systemach teleinformatycznych i sieciach, a zdolność wykrywania niepożądanych zdarzeń w infrastrukturze IT urzędu jest ograniczona. Brak zaawansowanej możliwości analizy logów i wykrywania anomalii na podstawie zautomatyzowanej analizy logów. W celu zmiany tej sytuacji, wnioskodawca planuje zakup systemu do zbierania i analizy logów z urządzeń sieciowych (UTM, switche), z funkcją zautomatyzowanej ich analizy i wykrywania potencjalnych incydentów bezpieczeństwa.
Koncepcja realizacji	W10, W17 - W chwili obecnej możliwości zapobiegania niechcianym zdarzeniom w infrastrukturze IT oraz ochrony danych są mocno ograniczone. Z posiadanych dwóch serwerów jeden jest stary (ok. 10 lat) i ulega coraz częstszym awariom (np. uszkodzenia dysków) powodującym czasowy brak dostępu do danych, drugi natomiast ma ograniczoną pojemność i nie może przejąć jego funkcji. Nie wszystkie switche w urzędzie posiadają wsparcie producenta (co stwarza ryzyko ograniczenia dostępu komputerów do sieci w przypadku awarii - brak możliwości wymiany). Urządzenie zabezpieczające sieć na jej brzegu jest stare, mało wydajne i nie posiada wsparcia, nie posiada też funkcjonalności kontrolera switchów, co utrudnia możliwość łatwego zarządzania dostępem do VLAN-ów. Oprogramowanie antywirusowe funkcjonuje, ale wygasają licencje na to oprogramowanie. W celu zmiany tego stanu rzeczy wnioskodawca planuje: - zakup nowego serwera z systemem operacyjnym Windows Server i licencjami dostępowymi; - zakup urządzenia UTM; - zakup 3 nowych switchów zarządzalnych (dwóch 48-portowych i 24-portowego), z możliwością łatwej integracji z zakupywanymi urządzeniami UTM (zarządzanie z poziomu UTM, jednolita administracja VLAN-ami); - zakup wyspecjalizowanego serwera plików (Network Attached Storage - NAS) umożliwiającego bezpieczne przechowywanie danych na dyskach

[redacted]

zorganizowanych w RAID - uszkodzenie jednego czy nawet dwóch dysków nie musi spowodować utraty danych ani nawet przerwy w pracy;
- zakup nowych licencji na oprogramowanie antywirusowe.

W05, W06, W12 - W chwili obecnej zabezpieczenia chroniące przed dostępem osób nieuprawnionych nie są centralnie zarządzane, co może powodować brak kontroli nad nimi, a proces zmiany uprawnień użytkowników jest utrudniony z uwagi na konieczność ich zmiany odrębnie na każdym z używanych przez nich komputerów i systemów. Istnieje wprawdzie domena Active Directory, ale nie obejmuje wszystkich komputerów w urzędzie - jedną z przyczyn niewdrożenia jej całkowicie był stary mało wydajny serwer powodujący problemy z logowaniem się do domeny. W celu zmiany tej sytuacji wnioskodawca planuje pełne wdrożenie Active Directory z centralną bazą użytkowników i podłączenie posiadanych komputerów do domeny AD. Do realizacji tego celu konieczny jest zakup nowego wydajnego serwera z systemem operacyjnym Windows Server i licencjami dostępowymi, służącego jako kontroler AD - może być to ta sama maszyna, która planowana jest do zakupu w celu migracji aplikacji używanych w urzędzie.

W16 - W chwili obecnej istnieje ryzyko utraty informacji związane z brakiem zasilania i będącym skutkiem tego nagłym wyłączeniem serwerów - zasilacze awaryjne są zużyte i nie są w stanie już podtrzymać wystarczająco długo działania kluczowych systemów. Kopie zapasowe są wprawdzie tworzone, ale brak systemu automatycznego backupu, ponadto na aktualnie używanych serwerach zaczyna brakować miejsca na kopie.

W celu zmiany tej sytuacji wnioskodawca planuje zakup nowego zasilacza awaryjnego (UPS) do serwerowni oraz zakup wyspecjalizowanego serwera plików (Network Attached Storage - NAS) o pojemności 12TB w przypadku konfiguracji dysków jako RAID5 z dyskiem zapasowym, na którym będą mogły być przechowywane kopie zapasowe przez dłuższy okres.

W27, W28 - W chwili obecnej czas przechowywania zapisów w systemach nie jest wystarczający z uwagi na brak miejsca na przechowywanie logów z wielu systemów. W celu zmiany tej sytuacji wnioskodawca planuje zakup dedykowanego urządzenia do zbierania logów głównie z urządzeń sieciowych (UTM, i switchów), ale również mogącego służyć jako serwer logów dla innych systemów obsługujących protokół syslog.

Zadanie: Poprawa bezpieczeństwa - obszar kompetencyjny

W05, W07 - W chwili obecnej zatrudniany pracownik IT nie jest wyszkolony z obsługi i konfiguracji planowanej do zakupu macierzy dyskowej, a w przypadku Active Directory ma jedynie podstawową wiedzę. W związku z tym wnioskodawca planuje przeszkolenie go w zakresie obsługi i konfiguracji zakupionej macierzy dyskowej oraz w zakresie konfiguracji i zarządzania AD pod kątem cyberbezpieczeństwa.

W07 - W chwili obecnej poziom świadomości w zakresie cyberbezpieczeństwa wśród pracowników urzędu nie jest wysoki. Istnieje dość wysokie ryzyko zajścia incydentów bezpieczeństwa z winy użytkownika. W celu zmiany tej sytuacji wnioskodawca planuje przeprowadzić kompleksowe szkolenie pracowników urzędu z cyberbezpieczeństwa, za pośrednictwem udostępnionej im platformy szkoleniowej online, które zaznajomi ich z potencjalnymi zagrożeniami i metodami przeciwdziałania im.

Projekt grantowy	Tak

2. Miejsce realizacji projektu

Obszar realizacji projektu (TERYT)	2608052
Maksymalna kwota dofinansowania grantu dla Beneficjenta (liczona po współczynniku dochodów Beneficjenta (w PLN)	352306,00
Minimalna wysokość wkładu własnego (wyrażona w %)	0,00
Procent dofinansowania UE (w %)	81,00
Procent dofinansowania BP (w %)	19,00
Województwo/Powiat/Gmina	ŚWIĘTOKRZYSKIE/pińczowski/Złota

3. Informacje o Grantobiorcy

NIP	6621750002
Nazwa Grantobiorcy	GMINA ZŁOTA
Regon	291010872
KRS	*brak danych*
Forma Prawna Grantobiorcy	WSPÓLNOTY SAMORZĄDOWE
Możliwość odzyskania VAT	Nie

Adres siedziby

Kraj	Polska
Miejscowość	Złota
Kod pocztowy	28-425
Ulica	ul. Sienkiewicza
Nr domu	79
Nr lokalu (opcjonalnie)	*nie dotyczy*
Adres e-mail	ug@gminazlota.pl
Adres ePUAP	/0117domwtd/SkrytkaESP
Nr tel	+48 413561601

Adres korespondencyjny

Adres korespondencyjny taki sam jak adres firmy	tak

Osoba upoważniona do kontaktu

Imię	
Nazwisko	
Stanowisko	

Adres e-mail	
Nr tel	
Nr rachunku bankowego Grantobiorcy	

Osoby upoważnione do reprezentacji Grantobi

Imię	
Nazwisko	
Stanowisko	
Podpis/kontrasygnata	
Adres e-mail	
Nr tel	

Imię	
Nazwisko	
Stanowisko	
Podpis/kontrasygnata	
Adres e-mail	
Nr tel	

4. Zakres rzeczowy projektu

Zadanie

Nazwa zadania	Poprawa bezpieczeństwa - obszar organizacyjny

Zadanie

Nazwa zadania	Poprawa bezpieczeństwa - obszar kompetencyjny

Zadanie

Nazwa zadania	Poprawa bezpieczeństwa - obszar techniczny

5. Zakres finansowy

Wydatki rzeczywiście ponoszone

Zadanie 1 - Poprawa bezpieczeństwa - 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	Wdrożenie SZBI	67 650,00	1	67 650,00	67 650,00	0,00	67 650,00	0,00
			SUMA	67 650,00	67 650,00	0,00	67 650,00	0,00

Zadanie 2 - Poprawa bezpieczeństwa - obszar kompetencyjny

Lp.	Nazwa kosztu	Cena jednostkowa (w PLN)	Liczba jednostek	Wydatki ogółem (w PLN)	Wydatki kwalifikowaln. e (w PLN)	Wydatki niekwalifikow . alne (w PLN)	Dofinansowa nie (w PLN)	Wkład własny (w PLN)
1	Szkolenie z cyberbezpiecz eństwa dla pracowników - 45 użytkowników , platforma edukacyjna	46 494,00	1	46 494,00	46 494,00	0,00	46 494,00	0,00
2	Szkolenie personelu IT z obsługi NAS	6 150,00	1	6 150,00	6 150,00	0,00	6 150,00	0,00
3	Szkolenie personelu IT z Active Directory	9 225,00	1	9 225,00	9 225,00	0,00	9 225,00	0,00
			SUMA	61 869,00	61 869,00	0,00	61 869,00	0,00

Zadanie 3 - Poprawa bezpieczeństwa - obszar techniczny

Lp.	Nazwa kosztu	Cena jednostkowa (w PLN)	Liczba jednostek	Wydatki ogółem (w PLN)	Wydatki kwalifikowaln e (w PLN)	Wydatki niekwalifikow alne (w PLN)	Dofinansowa- nie (w PLN)	Wkład własny (w PLN)
1	Urządzenie UTM	26 076,00	1	26 076,00	26 076,00	0,00	26 076,00	0,00
2	Zasilacz awaryjny - UPS	6 150,00	1	6 150,00	6 150,00	0,00	6 150,00	0,00
3	System do zbierania i analizy logów	77 843,01	1	77 843,01	77 843,01	0,00	77 843,01	0,00
4	Switch zarządzalny 48-portowy	12 361,50	2	24 723,00	24 723,00	0,00	24 723,00	0,00
5	Switch zarządzalny 24-portowy	11 750,19	1	11 750,19	11 750,19	0,00	11 750,19	0,00
6	Oprogramow anie antywirusowe - pakiet 45 licencji	7 380,00	1	7 380,00	7 380,00	0,00	7 380,00	0,00
7	NAS	18 450,00	1	18 450,00	18 450,00	0,00	18 450,00	0,00
8	Serwer	50 184,00	1	50 184,00	50 184,00	0,00	50 184,00	0,00
			SUMA	222 556,20	222 556,20	0,00	222 556,20	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	352 075,20	352 075,20	0,00	352 075,20	0,00

Podsumowanie budżetu

	Wydatki ogółem (w PLN)	Wydatki kwalifikowalne (w PLN)	Dofinansowanie (w PLN)
Razem w projekcie	352 075,20	352 075,20	352 075,20

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
352 075,20	352 075,20	352 075,20	100,00	285 181,05	81,00	19,00	66 894,15	0,00	0,00	0,00

7. Źródła finansowania wydatków (w PLN)

	Wydatki ogółem	Wydatki kwalifikowalne
Dofinansowanie	352 075,20	352 075,20
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	352 075,20	352 075,20

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 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
wybor_wojta_zaswiadczenie.pdf	145 KB	5749e5ec3833b49c2e35a6a09d6106c3df627fbc3db06b8b9c9e43d749f2fbe1
skarbnik_powolanie.pdf	153 KB	b676107af9ead8a2cf15bcc48aeeedf12ad53f0650573509652499101 9eb6eb3

Oświadczenie Grantobiorcy dot. VAT

Nazwa	Rozmiar	Suma kontrolna
oswiadczenie_vat_gmina_zlota.pdf	746 KB	b471b4a56d67dc85b00eb0f82f1f7355786699b680029379e1cec77224414fbc

Dodatkowe dokumenty ze strony Grantobiorcy

Nazwa	Rozmiar	Suma kontrolna
brak załączników		