

Systemowy identyfikator wniosku

118286e3-19eb-46f6-8778-2313a757d7d5

1. Informacje ogólne o projekcie

Data złożenia wniosku	2023-12-14 14:36:33
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	Bezpieczeństwo informacji na pierwszym planie: Cyberbezpieczna Gmina Gaworzycze
	<p>Cel Projektu: Wsparcie jednostki samorządu terytorialnego Gmina Gaworzycze w zakresie realizacji usług publicznych poprzez zwiększenie poziomu cyberbezpieczeństwa. Projekt ma na celu podniesienie kompetencji, organizacji oraz infrastruktury teleinformatycznej jednostki i jej podległych instytucji.</p> <p>Potrzeby Wnioskodawcy: Przeprowadzenie szczegółowej analizy potrzeb Wnioskodawcy związanych z cyfryzacją urzędu i jednostek podległych, z naciskiem na zwiększenie poziomu bezpieczeństwa informacji. W tym kontekście, identyfikacja obszarów wymagających natychmiastowych działań oraz długofalowych inwestycji. Analiza aktualnych zagrożeń cybernetycznych specyficznych dla sektora publicznego, z uwzględnieniem wyłączenia placówek ochrony zdrowia, mająca na celu dostosowanie działań projektowych do konkretnych ryzyk. Szkolenia dot. cyberbezpieczeństwa kierowane do pracowników JST i jednostek podległych, kadry zarządzającej i obsługi informatycznej. Zakup sprzętu i specjalistycznego oprogramowania w celu zwiększenia poziomu zabezpieczeń przed cyberatakami i ochrony informacji w zasobach JST i jednostek.</p> <p>Czas trwania: 2 lata, nie dłużej niż okres wskazany w umowie.</p> <p>Cele / efekty: Wdrażanie zaawansowanych technologii bezpieczeństwa informacyjnego w zgodności z zaleceniami Funduszy Europejskich. Zwiększenie efektywności działań administracji publicznej poprzez cyfryzację i optymalizację procesów. Podniesienie świadomości pracowników JST, jednostek i społeczności lokalnej w zakresie bezpieczeństwa cybernetycznego. Podniesienie poziomu bezpieczeństwa cyfrowego w kontekście ochrony danych osobowych i niezawodności systemów informatycznych Urzędu Gminy oraz jednostek podległych. Zwiększenie możliwości technicznych i organizacyjnych (w kontekście wydajności oraz bezpieczeństwa cyfrowego) w ujęciu nowych resortowych rozwiązań cyfrowych.</p> <p>Organizacyjny: W05; Konieczność przeprowadzania audytów cyberbezpieczeństwa Gmina realizuje przy udziale własnych środków. Koszty są względnie wysokie, jednak przy przyroście technologicznym w kwestii systemów informatycznych i mnogości stosowanych rozwiązań, wymagania audytorskie również wzrastają, co powoduje konieczność ponoszenia większych kosztów oraz doboru odpowiedniej jakości podmiotów zajmujących się kontrolą zagadnień audytowych. Planujemy przeprowadzenie kompleksowego audytu bezpieczeństwa teleinformatycznego jednostki samorządu oraz jej jednostek.</p>

Koncepcja realizacji

W02; UG dysponuje polityką bezpieczeństwa informacji oraz dokumentacją techniczną systemów informatycznych opracowaną na bazie doświadczenia z lat ubiegłych. Zamierzamy dokonać gruntownej analizy zastosowanej dokumentacji, poprzedzonej audytem i wprowadzenie zmian. Aktualizacja dokumentacji SZBI w UG umożliwi uzyskanie pożądanego poziomu bezpieczeństwa cyfrowego oraz rozbudowę istniejących rozwiązań związanych z kontrolą uprawnień użytkowników.

Ponadto szkoła nie posiada środków i przygotowania merytorycznego w zakresie stworzenia spójnego systemu zabezpieczeń w rozumieniu dokumentacji bezpieczeństwa informacji oraz wymogów resortowych (RODO oraz KRI). Stan obecny jest niezadowolający, co potwierdził ostatni audyt wewnętrzny. Niezbędne jest podjęcie gruntownych działań zmierzających do opracowania podstawowej dokumentacji kontrolującej obszar bezpieczeństwa i cyberbezpieczeństwa SZBI w SP W07; W chwili obecnej nie ma spójnego rozwiązania, które zapewniłoby Gminie i jednostkom skutecznego dostarczania informacji z zakresu bezpieczeństwa cyfrowego. Jednostki uczestniczą w szkoleniach prowadzonych przez służby IT i podmioty zajmujące się ochroną danych osobowych, jednak problemem jest brak możliwości dotarcia do większej ilości pracowników. Planujemy opracowanie i wdrożenie cyklicznego newslettera informacyjnego na temat zagrożeń cyberbezpieczeństwa dla pracowników UG oraz jednostek.

Kompetencyjne:

W07; Pomimo corocznych szkoleń zauważamy potrzebę większego informowania o zagrożeniach cyberbezpieczeństwa. Powodem, dla którego planuje się uruchomienie szkoleń jest stworzenie dodatkowego obszaru podnoszenia kompetencji i umożliwienie użytkownikom systemów informatycznych wymiany swoich doświadczeń z ekspertami w dziedzinie cyberbezpieczeństwa dla pracowników jednostki samorządu i jednostek

Lokalna służba IT podnosi kompetencje cyfrowe w ramach własnej inicjatywy, jednak nie posiadała możliwości uzyskania kwalifikacji związanych z obsługą incydentów, w tym również uzyskania gruntownej wiedzy z zakresu przestępczości cyfrowej. Planujemy szkolenia specjalistyczne dla informatyków i kadry zarządzającej w zakresie zastosowania środków bezpieczeństwa w myśl PBI - UG.

W02; Przygotowując się do zakupu urządzeń przeznaczonych do stworzenia profesjonalnej macierzy backupowej chroniącej zasoby Urzędu, planujemy skorzystanie ze wsparcia dostawców w zakresie zarówno użytkowania jak i rozwoju zakupionych rozwiązań informatycznych. Usługa w zakresie współpracy z zewnętrznymi ekspertami w zakresie wdrażania zakupionych rozwiązań, to jest instalacja nowych urządzeń infrastruktury informatycznej oraz agregacja i przeniesienie danych z istniejących rozwiązań w celu zachowania zgodności z opracowaną dokumentacją PBI - UG.

W22; Służba IT nie posiada obecnie kwalifikacji ISO 27001, postęp technologiczny i ilość systemów informatycznych użytkowanych w Urzędzie powoduje konieczność zwiększenia kompetencji w zakresie technicznym i organizacyjnym, które przyczynią się do ograniczenia kosztów działań zewnętrznych ekspertów. Szkolenie ISO 27001 podniesie kompetencję służby informatycznej w zakresie poprawy poziomu bezpieczeństwa i infrastruktury informatycznej przeznaczonej dla jednostek podległych pracujących na rozwiązaniach technicznych urzędu

Techniczny:

W16; UG i jednostki dysponują urządzeniami o parametrach niedostatecznie właściwych do stosowania systemów informatycznych, nie posiadają skutecznego rozwiązania zapewniającego zasilanie

awaryjne dla działania systemów informatycznych oraz urządzeń cyfrowych w sytuacjach krytycznych, większość stacji roboczych urzędu nie ma sprawnego systemu podtrzymania zasilania z uwagi na uszkodzenia zasilaczy spowodowanych zużyciem ogniw akumulatorowych, jednostki nie posiadają sprawnych urządzeń zapewniających zasilanie dla serwerów, w związku z często występującymi awariami istnieje ciągłe ryzyko utraty części danych z systemów dziedzinowych, żadna z jednostek nie ma skutecznie rozwiązanego sposobu na odmiejszczenie kopii cyfrowych danych. Urząd jest w posiadaniu prostych systemów archiwizacji danych składających się z serwerów plikowych oraz dysków sieciowych, mało wydajne dyski sieciowe typu NAS stosowane w jednostkach Gminy objętej projektem są niewszechogarnym środkiem ochrony cyfrowej w kontekście backupu danych. Niezbędna jest modernizacja i unowocześnienie infrastruktury teleinformatycznej poprzez zakup serwerów ZUK i GOPS, zakup systemu operacyjnego Microsoft Windows Server umożliwiającego stworzenie bezpiecznego systemu zarządzania uprawnieniami w związku z wdrażanym systemem dokumentacji PBI w SP, zakup agregatów/generatorów prądu oraz urządzenia mniejszej mocy przeznaczonego dla jednostek podległych i UG w sytuacjach awaryjnych, zakup UPS do kluczowych stacji roboczych do UG, zakup zasilaczy UPS do serwerów sieciowych do UG GOPS i ZUK, zakup dysków przenośnych na odmiejszczenie kopii danych UG i jednostki, macierz dyskowa przeznaczona do gromadzenia danych backup pochodzących z systemów informatycznych do UG, dyski sieciowe przeznaczone na dane cyfrowe typu backup dla UG i jednostek podległych Serwery umożliwią poprawę jakości i szybkości działania aplikacji dziedzinowych, co przełoży się na wzrost wydajności pracy jednostek. Zainstalowane na nich zostaną w nowsze wersje oprogramowania Microsoft Windows Server W17; W związku z charakterystyką pracy, w tym również pracy zdalnej, a także brakiem oczekiwanej niezawodności w działaniu poszczególnych stanowisk komputerowych czas działań służby informatycznej ulega wydłużeniu z uwagi na brak posiadania przez urząd stacji zapasowych, które mogłyby być użyte w przypadku awarii. Ponadto sieć teleinformatyczna nie ma potencjału do wdrożenia właściwego zabezpieczenia w kontekście nieuprawnionego dostępu do sieci oraz możliwości kontrolowania przepływu informacji wewnątrz instalacji, problemem jest również brak zasięgu urządzeń mobilnych oraz brak możliwości bezpiecznej pracy osób zewnętrznych. Obecnie posiadany certyfikat zabezpieczający witrynę internetową urzędu jest podstawowym modelem certyfikatu cyfrowego o niskim potencjale zapewniającym bezpieczeństwo. Urząd jest w posiadaniu rozwiązania antywirusowego Eset w podstawowym modelu ochrony, pozbawionego skutecznej odpowiedzi na szczególne zagrożenia cyfrowe jakim są złośliwe programy. W związku z tym niezbędny jest zakup urządzeń sieciowych aktywnych umożliwiających stosowanie bezpiecznej technologii VLAN w obrębie sieci Urzędu oraz jednostek podległych GOPS ZUK PP, zakup urządzenia typu Access Point umożliwiającego uruchomienie bezpiecznej sieci bezprzewodowej dla UG, certyfikat SSL niezbędny do zabezpieczenia połączenia na linii użytkownik-witryna Urzędu Gminy, zakup licencji na oprogramowanie antywirusowe dla UG.

Zasada równości:

Projekt jest neutralny pod względem płci, zapewniając równe szanse dla kobiet i mężczyzn zarówno w dostępie do szkoleń, jak i w korzystaniu z efektów projektu. Dodatkowo, infrastruktura i materiały projektowe spełniają standardy dostępności cyfrowej, co umożliwi dostępność dla osób z niepełnosprawnościami. Działania projektowe są elastyczne i mogą być dostosowane w celu eliminacji diagnozowanych nierówności.

	<p>Zgodność ze standardami dostępności: Projekt jest zgodny z obowiązującymi standardami dostępności dla polityk spójności - spełnianie kryteriów dostępności cyfrowej. Zakres oddziaływania: Projekt ma potencjał do zwiększenia poziomu cyberbezpieczeństwa nie tylko w samorządzie, ale także w lokalnym społeczeństwie poprzez edukację i podnoszenie świadomości w zakresie bezpieczeństwa informatycznego.</p>
Projekt grantowy	Tak

2. Miejsce realizacji projektu

Obszar realizacji projektu (TERYT)	0216022
Maksymalna kwota dofinansowania grantu dla Beneficjenta (liczona po współczynniku dochodów Beneficjenta (w PLN)	310940
Minimalna wysokość wkładu własnego (wyrażona w %)	0
Procent dofinansowania UE (w %)	82,0001
Procent dofinansowania BP (w %)	17,9999
Województwo/Powiat/Gmina	DOLNOŚLĄSKIE/polkowicki/Gaworzyce

3. Informacje o Grantobiorcy

NIP	6922255154
Nazwa Grantobiorcy	GMINA GAWORZYCE
Regon	390647587
KRS	<i>brak danych</i>
Forma Prawna Grantobiorcy	WSPÓLNOTY SAMORZĄDOWE
Możliwość odzyskania VAT	Nie

Adres siedziby

Kraj	Polska
Miejscowość	Gaworzyce
Kod pocztowy	59-180
Ulica	ul. Dworcowa
Nr domu	95
Nr lokalu (opcjonalnie)	<i>nie dotyczy</i>
Adres e-mail	ug@gaworzyce.com.pl
Adres ePUAP	/45ibv62lo3/skrytka
Nr tel	+48 768316285

Adres korespondencyjny

Adres korespondencyjny taki sam jak adres firmy	Tak
---	-----

Osoba upoważniona do kontaktu

Imię	Joanna
Nazwisko	Brodowska
Stanowisko	gł. spec. ds. współpracy lokalnej i promocji
Adres e-mail	j.brodowska@gaworzyce.com.pl
Nr tel	+48 768316285
Nr rachunku bankowego Grantobiorcy	68 8649 1060 2007 7001 1223 0034

Osoby upoważnione do reprezentacji Grantobiorcy

Imię	Jacek
Nazwisko	Szwagrzyk
Stanowisko	Wójt Gminy Gaworzyce
Podpis/kontrasygnata	podpis
Adres e-mail	wojt@gaworzyce.com.pl
Nr tel	+48 605839778

Imię	Anna
Nazwisko	Barylik
Stanowisko	Skarbnik Gminy Gaworzyce
Podpis/kontrasygnata	kontrasygnata
Adres e-mail	a.barylik@gaworzyce.com.pl
Nr tel	+48 768316285

4. Zakres rzeczowy projektu

Zadanie

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

Zadanie

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

Zadanie

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

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 sieciowy - do 2 jednostek podległych - ZUK i GOPS	12 500,00	2	25 000,00	25 000,00	0,00	25 000,00	0,00
2	Generator prądu 20kW	45 000,00	1	45 000,00	45 000,00	0,00	45 000,00	0,00
3	Generator prądu 8kW	8 000,00	1	8 000,00	8 000,00	0,00	8 000,00	0,00
4	Dysk twardy do serwera archiwizacyjnego NAS - ZUK, GOPS, UG, PP	1 000,00	4	4 000,00	4 000,00	0,00	4 000,00	0,00
5	Dysk przenośny USB 2TB - ZUK, PP, SP, GOPS, UG	400,00	5	2 000,00	2 000,00	0,00	2 000,00	0,00
6	Serwer archiwizacyjny NAS - ZUK, GOPS, UG, PP	1 000,00	4	4 000,00	4 000,00	0,00	4 000,00	0,00
7	Acces point - Urząd Gminy	1 200,00	1	1 200,00	1 200,00	0,00	1 200,00	0,00
8	Certyfikat SSL - Urząd Gminy	500,00	1	500,00	500,00	0,00	500,00	0,00
9	Macierz dyskowa - Urząd Gminy	17 000,00	1	17 000,00	17 000,00	0,00	17 000,00	0,00
10	Dyski twarde do macierzy dyskowej - UG	1 000,00	10	10 000,00	10 000,00	0,00	10 000,00	0,00
11	UPS - zasilacze awaryjne do kluczowych stacji roboczych - UG	440,00	6	2 640,00	2 640,00	0,00	2 640,00	0,00
12	UPS - zasilacze awaryjne do serwerów - ZUK, GOPS, UG	1 000,00	3	3 000,00	3 000,00	0,00	3 000,00	0,00

13	System operacyjny niezbędny do instalacji i utrzymania systemów bezpieczeństwa - Szkoła Podstawowa	12 000,00	1	12 000,00	12 000,00	0,00	12 000,00	0,00
14	Przełącznik sieciowy zarządzany z obsługą VLAN, MACses, standardu 802.1X - GOPS, ZUK, PP	920,00	3	2 760,00	2 760,00	0,00	2 760,00	0,00
15	Oprogramowanie antywirusowe dla Gminy Gaworzyce - Urząd - na 2 lata	5 000,00	1	5 000,00	5 000,00	0,00	5 000,00	0,00
16	Licencja na oprogramowanie dostępne pulpitu zdalnego RDP na potrzeby rozbudowy istniejącego systemu bezpieczeństwa w Urzędzie	30 000,00	1	30 000,00	30 000,00	0,00	30 000,00	0,00
17	Serwer sieciowy do obsługi pulpików wirtualnych z oprogramowaniem serwerowym - Gmina Gaworzyce - Urząd	41 000,00	1	41 000,00	41 000,00	0,00	41 000,00	0,00
			SUMA	213 100,00	213 100,00	0,00	213 100,00	0,00

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	Organizacja szkoleń stacjonarnych dedykowanych dla pracowników JST i jednostek podległych posiadające stosowną wiedzę oraz min. 2-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń wzmacniających świadomość cyberzagrożeń - dla 5	5 500,00	5	27 500,00	27 500,00	0,00	27 500,00	0,00
2	Szkolenie dla Informatyka w zakresie 270001 - szkolenie specjalistyczne w zakresie planowanych do zastosowania środków bezpieczeństwa	6 000,00	1	6 000,00	6 000,00	0,00	6 000,00	0,00
3	Usługa współpracy z zewnętrznymi ekspertami w zakresie wdrażania zakupionych rozwiązań - 32 godziny	160,00	32	5 120,00	5 120,00	0,00	5 120,00	0,00

4	Szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli i kadry JST istotnych z punktu widzenia wdrażanej PBI	1 600,00	2	3 200,00	3 200,00	0,00	3 200,00	0,00
			SUMA	41 820,00	41 820,00	0,00	41 820,00	0,00

Zadanie 3 - 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	Przygotowanie newslettera dla pracowników upowszechniającego świadomość o zagrożeniach cybernetycznych - kierowane do 5 jednostek	1 500,00	1	1 500,00	1 500,00	0,00	1 500,00	0,00
2	Opracowanie i wdrożenie SZBI w Szkole Podstawowej w Gaworzycach	4 000,00	1	4 000,00	4 000,00	0,00	4 000,00	0,00
3	Audyty zgodności z KRI	6 000,00	5	30 000,00	30 000,00	0,00	30 000,00	0,00
4	Aktualizacja dokumentacji SZBI w Urzędzie Gminy w Gaworzycach	2 400,00	1	2 400,00	2 400,00	0,00	2 400,00	0,00
			SUMA	37 900,00	37 900,00	0,00	37 900,00	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	292 820,00	292 820,00	0,00	292 820,00	0,00

Podsumowanie budżetu

	Wydatki ogółem (w PLN)	Wydatki kwalifikowalne (w PLN)	Dofinansowanie (w PLN)
Razem w projekcie	292 820,00	292 820,00	292 820,00

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
292 820,00	292 820,00	292 820,00	100	240 112,59	82	18	52 707,41	0,00	0,00	0

7. Źródła finansowania wydatków (w PLN)

	Wydatki ogółem	Wydatki kwalifikowalne
Dofinansowanie	292 820,00	292 820,00
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	292 820,00	292 820,00

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 przestania 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 o wyborze wójta-sig.pdf	671 KB	9988951961df8abff03fe8d39497e71799fb5cb21ee022c1f98547a023a58366
Uchwała o powołaniu skarbnika-sig.pdf	196 KB	a21d9a530e6d74f87e6b904a071c175b9cbc2a05433f7e3c2c295e3c34a08fbc

Oświadczenie Grantobiorcy dot. VAT

Nazwa	Rozmiar	Suma kontrolna
OŚWIADCZENIE_O_VAT-sig-sig.pdf	11 MB	6cc13bda7ec0c814143f4cf6692767356ea1f560c116dbceb030a8726a90e3e2

Dodatkowe dokumenty ze strony Grantobiorcy

Nazwa	Rozmiar	Suma kontrolna
Szkoła Podstawowa Uchwała +Statut-sig.pdf	25 MB	655529965f05f8b20a19c3cf9262f414e26d2b5283dc375bfc01b13649b20c8e
GOPS, ZUK, PP statuty, uchwały.pdf	22 MB	c79025d4023e541d676cfffad0efd1eab2b87894e8c0484935818c882b84e5d4d