Systemowy identyfikator wniosku	3939afb1-59d4-4d85-bd63-8fa0b7303bc8

1. Informacje ogólne o projekcie

Data złożenia wniosku	2025-10-02 11:43:30
Program	Krajowy Plan Odbudowy i Zwiększania Odporności
Priorytet	C3 Cyberbezpieczeństwo
Działanie	C3.1.1. Cyberbezpieczeństwo - CyberPL
Fundusz	Krajowy Plan Odbudowy i Zwiększania Odporności
Numer naboru	KPOD.05.10-CW.01-001/25
Tytuł projektu	Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Pleszewie poprzez wdrożenie nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie kompetencji personelu.
Krótki opis projektu	Przedsiębiorstwo Komunalne Sp. z o.o. w Pleszewie zidentyfikowała potrzebę zwiększenia poziomu bezpieczeństwa informacji. Analiza ryzyka, przeprowadzona w świetle planowanych wymogów nowelizacji UKSC (NIS2), wykazała kluczowe obszary wymagające modernizacji. Najważniejszym z nich jest zabezpieczenie sieci OT, która jest fundamentem ciągłości dostaw wody. Dotychczasowe rozwiązania nie zapewniają pełnej segmentacji, monitorowania i ochrony przed cyberzagrożeniami. Dodatkowo, analiza ujawniła potrzebę podniesienia kompetencji personelu. Projekt ma na celu wzmocnienie cyberodporności poprzez modernizację infrastruktury oraz rozwój kompetencji zespołów. W ramach projektu zrealizowane zostaną działania: 1.Modernizacja infrastruktury sieciowej: Wdrożenie segmentacji i mikrosegmentacji sieci IT/OT, co umożliwi izolację newralgicznych systemów i minimalizację potencjalnych szkód w przypadku ataku. Zostanie wdrożony system monitorowania ruchu sieciowego (IDS/IPS). Umożliwi on gromadzenie logów systemowych i dowodów cyfrowych niezbędnych do analizy incydentów. 2.Wdrożenie bezpiecznych zdalnych dostępów: Wprowadzenie scentralizowanego i bezpiecznego systemu zdalnego dostępu, który pozwoli na kontrolę i audytowanie połączeń z sieciami OT/IT. 3.Zapewnienie ciągłości działania: Zostanie wdrożony system do tworzenia i zarządzania kopiami zapasowymi, w tym również dla systemów sterowania, co zapewni szybki powrót do sprawności w przypadku incydentu. 4.Rozwój kompetencji: Zaplanowano cykl szkoleń dla całego personelu podnoszący świadomość i umiejętności w zakresie cyberbezpieczeństwa. Projekt jest zgodny z priorytetami KPO i Zwiększania Odporności, a w szczególności z celem Transformacji Cyfrowej. Inwestycja w nowoczesne technologie cyberbezpieczeństwa jest kluczowym elementem w dążeniu do stworzenia bezpiecznej infrastruktury krytycznej, zapewniającej ciągłość świadczenia usług publicznych. Data rozpoczęcia projektu: 23.09.2025 Data zakończenia projektu: 30.06.2026
Projekt grantowy	Tak

2. Miejsce realizacji projektu

Czy projekt jest realizowany na terenie całego kraju?	Nie	
Województwo	Powiat	Gmina
WIELKOPOLSKIE	pleszewski	Pleszew (miasto)

3. Informacje o Grantobiorcy

NIP	6170013743
Nazwa Grantobiorcy	PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Regon	250423184
KRS	0000192188
Forma prawna Grantobiorcy	SPÓŁKI Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Forma własności	Jednostki samorządu terytorialnego lub samorządowe osoby prawne
Krótki opis Grantobiorcy	Przedsiębiorstwo Komunalne Sp. z o.o. w Pleszewie jest spółką użyteczności publicznej, której jedynym właścicielem jest Gmina Pleszew. Działamy od wielu lat jako kluczowy podmiot odpowiedzialny za realizację zadań w zakresie gospodarki komunalnej, ze szczególnym naciskiem na zbiorowe zaopatrzenie mieszkańców w wodę oraz odprowadzanie i oczyszczanie ścieków. Nasza działalność obejmuje utrzymanie i rozbudowę infrastruktury wodociągowej i kanalizacyjnej, co ma bezpośredni wpływ na jakość życia społeczności lokalnej. Spółka obsługuje zarówno gospodarstwa domowe, jak i podmioty gospodarcze, dbając o niezawodność dostaw wody oraz bezpieczeństwo procesów oczyszczania ścieków. W trosce o mieszkańców oraz środowisko naturalne regularnie inwestujemy w modernizację systemów technologicznych i wdrażamy rozwiązania przyjazne środowisku. Naszą misją jest świadczenie usług na najwyższym poziomie, w oparciu o zasady efektywności, odpowiedzialności społecznej i zrównoważonego rozwoju. Równolegle koncentrujemy się na wzmacnianiu bezpieczeństwa funkcjonowania przedsiębiorstwa zarówno w obszarze technicznym, jak i cyfrowym. Inwestycje w nowoczesne technologie i szkolenia pracowników pozwalają nam sprostać współczesnym wyzwaniom, zapewnić ciągłość działania oraz chronić dane mieszkańców gminy Pleszew
Rodzaj Grantobiorcy	przedsiębiorstwo wodociągowo-kanalizacyjne
Okres utrzymania efektów projektu	3
Typ Grantobiorcy	Przedsiębiorstwa wodociągowo-kanalizacyjne
Wielkość przedsiębiorstwa	Nie dotyczy
Dominujący kod PKD	3600Z

Adres siedziby

Kraj	Polska
Miejscowość	Pleszew
Kod pocztowy	63-300

Ulica	ul. Polna
Nr domu	71
Nr lokalu	*brak danych*
Adres e-mail	pk.pleszew@post.pl
Adres ePUAP	/PK_Pleszew/skrytkaESP
Adres do eDoręczeń	AE:PL-77305-49739-DJEAA-19
Telefon	+48 627421664

Adres korespondencyjny

Adres korespondencyjny taki sam jak adres siedziby	Tak
Ulica	*brak danych*

Osoba upoważniona do kontaktu

Imię	Małgorzata
Nazwisko	Urban
Stanowisko	Kierownik Jednostki Realizującej Projekt
Adres e-mail	malgorzataurban@pkpleszew.pl
Telefon	+48 627412326

4. Lista mierzalnych wskaźników projektu

Wskaźniki horyzontalne

Wskaźniki rezultatu

Jednostka miary	Wartość bazowa	Wartość docelowa	Podział na płeć	Wartość bazowa K	Wartość bazowa M	Wartość docelowa K	Wartość docelowa M
przedsiębiorstwa	0,0000	0,0000	Nie	*nie dotyczy*	*nie dotyczy*	*nie dotyczy*	*nie dotyczy*
Nazwa wskaźnika: Przedsiębiorstwa objęte wsparciem na opracowywanie lub przyjmowanie produktów, usług i procesów cyfrowych							
Sposób pomiaru: nie dotyczy							

Jednostka miary	Wartość bazowa	Wartość docelowa	Podział na płeć	Wartość bazowa K	Wartość bazowa M	Wartość docelowa K	Wartość docelowa M
przedsiębiorstwa	0,0000	0,0000	Nie	*nie dotyczy*	*nie dotyczy*	*nie dotyczy*	*nie dotyczy*
Nazwa wskaźnika: Przedsiębiorstwa objęte wsparciem (w tym: małe, również mikro, średnie, duże)							
Sposób pomiaru: nie dotyczy							

Jednostka miary	Wartość bazowa	Wartość docelowa	Podział na płeć	Wartość bazowa K	Wartość bazowa M	Wartość docelowa K	Wartość docelowa M
użytkownicy /rok	0,0000	38,0000	Tak	0,0000	0,0000	22,0000	16,0000

Nazwa wskaźnika: Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych
Sposób pomiaru: Pomiar nastąpi na podstawie list obecności ze szkoleń z zakresu cyberbezpieczeństwa. Dodatkowo, wskaźnik będzie mierzony na podstawie ewidencji użytkowników posiadających dostęp do zmodernizowanych lub nowo wdrożonych systemów cyfrowych (np. systemów do zdalnych dostępów, monitorowania infrastruktury IT/OT).

Wskaźniki własne

Wskaźniki produktu

Jednostka miary	Wartość bazowa	Wartość docelowa	Podział na płeć
liczba	0,0000	1,0000	Nie
Nazwa wskaźnika: Liczba podmiotów objętych wsparciem			
Sposób pomiaru: Wskaźnik zostanie zweryfikowany na podstawie umowy o dofinansowanie projektu zawartej pomiędzy Skarbem Państwa, w imieniu którego działa Centrum Projektów Polska Cyfrowa a Przedsiębiorstwem Komunalnym Sp. z o.o. w Pleszewie.			

5. Wpływ projektu na zasady horyzontalne

Wpływ projektu na zasady horyzontalne

Zgodność z zasadami horyzontalnymi	Czy projekt jest zgodny z zasadą horyzontalną	Uzasadnienie

Czy projekt grantowy będzie zgodny z zasadą „niewyrządzania znaczącej szkody środowisku" (DNSH – „do no significant harm")?	Tak	Projekt jest w pełni zgodny z zasadą DNSH. Zaplanowane działania zostały zaprojektowane, aby minimalizować negatywny wpływ na środowisko, a nawet pozytywnie na nie oddziaływać. Inwestycja dotyczy wyłącznie zakupu i wdrożenia oprogramowania oraz nowoczesnych urządzeń IT/OT, takich jak serwery. Nie są przewidziane żadne prace budowlane, co eliminuje negatywny wpływ na bioróżnorodność i ekosystemy oraz emisje zanieczyszczeń. Minimalizacja negatywnego wpływu: Efektywność energetyczna: Wszystkie nowo zakupione urządzenia będą posiadały certyfikaty wysokiej efektywności energetycznej (np. Energy Star, EPEAT). Zoptymalizuje to zużycie energii i przyczyni się do redukcji śladu węglowego firmy. Gospodarka odpadami: Wycofany z użytku sprzęt elektroniczny zostanie przekazany do wyspecjalizowanych podmiotów zajmujących się recyklingiem, zgodnie z obowiązującymi przepisami. Pozytywny wpływ na środowisko: Ochrona zasobów wodnych: Wzmocnienie cyberbezpieczeństwa sieci wodociągowej i systemów OT bezpośrednio przekłada się na zwiększenie kontroli nad infrastrukturą. Umożliwi to skuteczne zapobieganie awariom, wyciekom lub skażeniom, które mogłyby mieć katastrofalny wpływ na zasoby wodne i lokalne ekosystemy. Wdrożenie monitoringu i zabezpieczeń zmniejsza ryzyko cyberataków, które mogłyby doprowadzić do strat wody lub skażenia. Podsumowując, projekt nie tylko nie wyrządza szkody środowisku, ale aktywnie przyczynia się do jego ochrony, co jest kluczowe w sektorze wodociągowym.

Czy projekt grantowy zapewnia zgodność z zasadą zrównoważonego rozwoju - racjonalne wykorzystywanie zasobów naturalnych?	Tak	Projekt jest w pełni zgodny z zasadą zrównoważonego rozwoju, a jego realizacja będzie oparta na racjonalnym wykorzystaniu zasobów naturalnych oraz minimalizacji negatywnego wpływu na środowisko. Racjonalne wykorzystanie zasobów: Efektywność energetyczna i ograniczenie emisji: W ramach projektu zostanie zakupiony wyłącznie sprzęt o wysokiej efektywności energetycznej, posiadający międzynarodowe certyfikaty, takie jak Energy Star. Wybór takich urządzeń zminimalizuje zużycie energii i bezpośrednio przyczyni się do redukcji emisji dwutlenku węgla. Trwałość i minimalizacja odpadów: Wybrany sprzęt będzie charakteryzował się długim cyklem życia i wsparciem producenta, co ograniczy konieczność jego częstej wymiany i tym samym zmniejszy ilość generowanych odpadów elektronicznych. Gospodarka obiegu zamkniętego: Wycofany z użytku sprzęt elektroniczny zostanie przekazany do wyspecjalizowanych podmiotów zajmujących się jego recyklingiem, zgodnie z obowiązującymi przepisami. Pozytywny wpływ na środowisko: Ochrona kluczowych zasobów wodnych: Projekt przyczyni się do zwiększenia bezpieczeństwa systemów zarządzających siecią wodno-kanalizacyjną, w tym stacjami uzdatniania i oczyszczalni ścieków. Zwiększona cyberodporność ograniczy ryzyko ataków mogących prowadzić do skażenia wody, niekontrolowanych wycieków, przerw w dostawach lub degradacji jakości wody. Działania te będą miały bezpośredni, pozytywny wpływ na ochronę zasobów wodnych oraz zapobieganie zagrożeniom środowiskowym.

Czy realizacja projektu grantowego gwarantuje zachowanie zgodności z zasadą równości szans i niedyskryminacji oraz zasadą równości szans kobiet i mężczyzn?	Tak	Projekt w pełni gwarantuje zachowanie zgodności z zasadą równości szans i niedyskryminacji, w tym równości kobiet i mężczyzn, a także dostępności dla osób z niepełnosprawnościami. Wnioskodawca stosuje politykę równego traktowania na wszystkich etapach realizacji. Wnioskodawca zapewnia: Równy dostęp do stanowisk i rozwoju: Firma promuje udział kobiet w działach technicznych i zapewnia równe szanse w dostępie do stanowisk i rozwoju zawodowego, co jest zgodne z wewnętrzną polityką równościową i antymobbingową. Uniwersalne projektowanie: Realizowane w ramach projektu rozwiązania cyfrowe będą zgodne z zasadami uniwersalnego projektowania, zapewniając ich intuicyjność i dostępność dla wszystkich użytkowników, niezależnie od ich sprawności. Dostosowanie komunikacji: Wszystkie materiały informacyjne i szkoleniowe będą wolne od stereotypów płciowych i dostosowane do zasad dostępności, w tym czytelności, kontrastu i wielkości czcionki. Komunikacja dotycząca projektu będzie prowadzona w sposób włączający i inkluzywny. Powszechny dostęp do szkoleń: Wszyscy pracownicy i pracownice będą mieli równy dostęp do szkoleń z zakresu cyberbezpieczeństwa. Ich forma i przekaz zostaną dostosowane tak, aby były zrozumiałe i dostępne dla każdego, co jest kluczowe dla budowania równych kompetencji w organizacji. Realizacja i rezultaty projektu będą dostępne dla wszystkich z poszanowaniem zasad równości i niedyskryminacji.

6. Zakres rzeczowy projektu

Zadanie 1 Obszar organizacyjny

Nazwa zadania	Obszar organizacyjny

Opis działań planowanych do realizacji w ramach wskazanych zadań /czas realizacji/podmiot działania	Spółka zidentyfikowała pilną potrzebę wzmocnienia cyberbezpieczeństwa. Realizacja działań w obszarze organizacyjnym stanowi fundament dla osiągnięcia cyberodporności, zgodnie z celami konkursu i wytycznymi Krajowego Planu Odbudowy (KPO). Działania te są niezbędne do formalizacji procesów i obiektywnej oceny stanu bezpieczeństwa w organizacji, obejmując zarówno systemy IT, jak i krytyczne dla ciągłości dostaw wody systemy OT. Doradztwo kontraktowe (zadanie 1.1.13): Opracowanie wzorcowych zapisów umownych, które zabezpieczą spółkę przed ryzykami płynącymi z łańcucha dostaw i zewnętrznych usług, w tym zdalnych dostępów i monitorowania. Działania te pozwolą zminimalizować ryzyko zewnętrzne, co jest kluczowym wymogiem dla podmiotów kluczowych. Uzasadnienie dla Audytu Systemu Zarządzania Bezpieczeństwem Informacji - Zadania U25 i U37 Audyty stanowią kluczowy mechanizm obiektywnej oceny stanu bezpieczeństwa i są niezbędne dla ciągłego doskonalenia. Realizacja zadania 1.1.2. Audyt Systemu Zarządzania Bezpieczeństwem Informacji jest zgodna z kategoriami U25 i U37 KPO. Audyt bezpieczeństwa: Przeprowadzenie kompleksowego audytu wewnętrznego/zewnętrznego przez niezależny podmiot z certyfikatami w zakresie cyberbezpieczeństwa. Audyt ten pozwoli na weryfikację polityk i procedur pod kątem ich skuteczności i zgodności z normami (ISO 27001, NIS2). Audytorzy dokonają oceny stopnia wdrożenia kontroli technicznych, wskażą luki i zidentyfikują obszary do natychmiastowej poprawy. Audyt zgodności z przepisami: Szczegółowa analiza zgodności działania spółki z planowaną nowelizacją UKSC dla podmiotów kluczowych i ważnych. Weryfikacja obejmie kluczowe obszary, takie jak zarządzanie incydentami, zarządzanie ryzykiem oraz raportowanie. Data rozpoczęcia projektu: 23.09.2025 Data zakończenia projektu: 30.06.2026
Wydatki rzeczywiście ponoszone	Tak
Uproszczona metoda rozliczania	Nie
Czy rozliczane jako koszty pośrednie	Nie

Zadanie 2 Obszar kompetencyjny

Nazwa zadania	Obszar kompetencyjny

Opis działań planowanych do realizacji w ramach wskazanych zadań /czas realizacji/podmiot działania	Realizacja projektu grantowego koncentruje się nie tylko na modernizacji technologicznej, ale także na kluczowym obszarze, jakim jest rozwój kompetencji personelu. Wzmocnienie bezpieczeństwa przedsiębiorstwa wodociągowego wymaga podniesienia świadomości i umiejętności pracowników na wszystkich szczeblach - od kadry zarządzającej, przez specjalistów IT/OT, aż po wszystkich użytkowników systemów. Działania te są zgodne z celami Krajowego Planu Odbudowy (KPO). Planowane działania szkoleniowe Szkolenia dla kadry kierowniczej (zadanie 2.1.2, kategoria U27) Opis: Dwudniowe szkolenie w centrum edukacyjnym, które ma na celu podniesienie świadomości kadry zarządzającej w zakresie cyberbezpieczeństwa. Szkolenie skupi się na aspekcie strategicznym, ryzyku biznesowym i wymaganiach regulacyjnych. Kadra kierownicza zdobędzie wiedzę o tym, jak cyberbezpieczeństwo wpływa na ciągłość działania firmy i jak zarządzać ryzykiem w kontekście incydentów. Podmiot odpowiedzialny: Zewnętrzna firma szkoleniowa. Szkolenia specjalistyczne (zadanie 2.1.3, kategoria U28) Opis: Dwudniowe szkolenie w centrum edukacyjnym, dedykowane kadrze zarządzającej i specjalistom IT/OT. Uczestnicy zdobędą praktyczną wiedzę na temat wdrożonych lub planowanych do wdrożenia środków bezpieczeństwa. Szkolenie zapewni umiejętności niezbędne do efektywnego wykorzystywania narzędzi, takich jak systemy monitorujące czy systemy zarządzania incydentami. Podmiot odpowiedzialny: Zewnętrzna firma szkoleniowa. Szkolenia z testami socjotechnicznymi (zadanie 2.1.4, kategoria U29) Opis: Szkolenia z wykorzystaniem technologii VR (wirtualna rzeczywistość), które odbędą się w siedzibie Spółki. Celem jest praktyczna weryfikacja świadomości zagrożeń socjotechnicznych, takich jak phishing czy spoofing, oraz ocena reakcji personelu. Szkolenia te pozwolą na identyfikację luk w wiedzy i dopasowanie procedur reagowania, zwłaszcza w przypadku kluczowych pracowników i specjalistów odpowiedzialnych za SZBI. Podmiot odpowiedzialny: Zewnętrzna firma szkoleniowa, specjalizująca się w nowoczesnych metodach weryfikacji kompetencji. Uzasadnienie potrzeby działań: Powyższe działania stanowią spójny i kompleksowy plan podniesienia kompetencji w organizacji. Szkolenia dla kadry kierowniczej zapewnią strategiczne zrozumienie ryzyka, podczas gdy szkolenia specjalistyczne dostarczą konkretnych narzędzi i umiejętności operacyjnych. Co więcej, weryfikacja wiedzy poprzez testy socjotechniczne z użyciem technologii VR pozwoli na bieżąco dostosowywać politykę bezpieczeństwa do realnych zagrożeń. Inwestycja w rozwój kompetencji personelu jest nie tylko wymogiem regulacyjnym, ale także najefektywniejszą formą obrony przed atakami, które coraz częściej celują w ludzki czynnik. Data rozpoczęcia projektu: 23.09.2025 Data zakończenia projektu: 30.06.2026
Wydatki rzeczywiście ponoszone	Tak
Uproszczona metoda rozliczania	Nie
Czy rozliczane jako koszty pośrednie	Nie

Zadanie 3 Obszar techniczny IT

Nazwa zadania	Obszar techniczny IT

Opis działań planowanych do realizacji w ramach wskazanych zadań /czas realizacji/podmiot działania	Przedsiębiorstwo Komunalne Sp. z o.o. w Pleszewie uznaje, że kluczowym elementem podniesienia cyberodporności jest kompleksowa modernizacja środowiska teleinformatycznego IT, zgodnie z wymaganiami dyrektywy NIS2. Projekt zakłada wdrożenie nowoczesnych rozwiązań sprzętowych i programowych, które w pełni zabezpieczą infrastrukturę oraz dane biznesowe. 1. Ochrona punktów końcowych i danych, zabezpieczenie stacji roboczych i serwerów to priorytet. W ramach projektu przewidziano zakup i wdrożenie: Oprogramowania do zarządzania podatnościami (O35). Narzędzie to umożliwi ciągłe skanowanie, wykrywanie i automatyczne usuwanie luk w oprogramowaniu, co jest kluczowe dla minimalizacji ryzyka ataków. Systemów do ochrony przed ransomware (O40) oraz EDR (3.1.8, O40). Rozwiązania te zapewnią wielowarstwową ochronę punktów końcowych, izolując potencjalnie szkodliwe oprogramowanie i reagując na zaawansowane zagrożenia w czasie rzeczywistym. Oprogramowania do zarządzania tożsamością i dostępem (O31) i systemów MFA (O43). Rozwiązania te wzmocnią kontrolę dostępu do krytycznych zasobów, minimalizując ryzyko nieautoryzowanych działań. Systemu DLP (O26). Oprogramowanie to ma na celu ochronę przed wyciekiem poufnych danych. 2. Zabezpieczenie infrastruktury sieciowej i serwerowej. Wdrożenie nowoczesnych urządzeń sieciowych i serwerów jest fundamentem cyberbezpieczeństwa. Planowane działania to: Systemy Firewall, WAF, UTM, NDR (S02, O14). Wdrożenie tych rozwiązań umożliwi kompleksowe zabezpieczenie brzegów sieci, segmentację i monitorowanie ruchu w poszukiwaniu anomalii i ataków sieciowych. Switch z obsługą VLAN i WPA3 (S27, S34). Urządzenia te pozwolą na logiczną segmentację sieci, co znacznie ograniczy potencjalne szkody w przypadku ataku. Serwery fizyczne (S13). Nowe serwery zapewnią stabilne i wydajne środowisko dla wdrożenia systemów bezpieczeństwa. Stacja przesiadkowa (S35). Stacja ta będzie stanowiła bezpieczny punkt dostępowy do krytycznych systemów, minimalizując ryzyko kompromitacji. System SIEM (S04). Zintegrowany system do zarządzania informacjami i zdarzeniami bezpieczeństwa umożliwi centralne monitorowanie i korelację zdarzeń z obu obszarów. Systemy do tworzenia kopii zapasowych (S14). Wdrożenie serwera NAS zapewni skuteczną ochronę przed utratą danych i umożliwi szybkie przywrócenie systemów po ataku, np. ransomware. 3. Usługi wdrożenia i utrzymania. Skuteczność zakupionych rozwiązań zależy od ich profesjonalnego wdrożenia. Projekt przewiduje profesjonalne usługi (U18, U39, U41) w zakresie instalacji, konfiguracji i hardeningu systemów. Dodatkowo, usługa MDR (U11) zapewni stały nadzór nad bezpieczeństwem, a końcowy audyt (U37) zweryfikuje poprawność wdrożenia. Podsumowując, realizacja tych zadań ma kluczowe znaczenie dla spełnienia wymogów NIS2, zapewnienia ciągłości działania oraz podniesienia ogólnego poziomu cyberodporności Spółki. Data rozpoczęcia projektu: 23.09.2025 Data zakończenia projektu: 30.06.2026
Wydatki rzeczywiście ponoszone	Tak
Uproszczona metoda rozliczania	Nie
Czy rozliczane jako koszty pośrednie	Nie

Zadanie 4 Obszar techniczny OT

Nazwa zadania	Obszar techniczny OT
Opis działań planowanych do realizacji w ramach wskazanych zadań /czas realizacji/podmiot działania	Projekt w obszarze technicznym OT jest kluczowy dla zabezpieczenia infrastruktury krytycznej spółki wodociągowej. Systemy Operational Technology (OT), które sterują procesami uzdatniania i dystrybucji wody, są coraz częściej celem ataków cybernetycznych, stanowiąc poważne zagrożenie dla ciągłości dostaw i bezpieczeństwa publicznego. Ich kompleksowa ochrona jest priorytetem. W celu zapewnienia pełnej cyberodporności sieci OT, projekt przewiduje wdrożenie zintegrowanych i zaawansowanych systemów bezpieczeństwa. Planowane działania to: Wielofunkcyjne systemy bezpieczeństwa OT (OT3). Te zaawansowane urządzenia będą stanowić pierwszą i najistotniejszą barierę ochronną, kontrolując ruch w sieciach OT i blokując nieautoryzowane próby dostępu do sterowników i serwerów procesowych. Ich wdrożenie zapewni bezpieczeństwo na poziomie fizycznej warstwy sieci. Oprogramowanie All-in-One (O08). To unikalne rozwiązanie zintegruje w jednej platformie kluczowe funkcjonalności, takie jak MDR (Managed Detection and Response), SIEM (Security Information and Event Management), IDS (Intrusion Detection System) oraz NDR (Network Detection and Response). Takie kompleksowe podejście umożliwi centralne monitorowanie, korelację zdarzeń i błyskawiczne reagowanie na wszelkie anomalie i ataki w sieci OT, co jest niemożliwe w przypadku rozproszonych systemów. System do zarządzania tożsamością i dostępem (O31). Wdrożenie tego narzędzia zapewni, że dostęp do krytycznych systemów OT będzie możliwy wyłącznie dla uprawnionego personelu, co znacznie minimalizuje ryzyko nieautoryzowanych działań, wynikających np. z kradzieży tożsamości. Zapewnienie ciągłości działania i odporności. Aby zagwarantować nieprzerwaną pracę infrastruktury, projekt uwzględnia następujące rozwiązania: Systemy zasilania awaryjnego (Z21). Zasilacze UPS zabezpieczą kluczowe urządzenia bezpieczeństwa przed skutkami nagłych przerw w zasilaniu. System do tworzenia kopii zapasowych (S21). Wdrożenie serwera NAS pozwoli na regularne tworzenie kopii zapasowych danych i konfiguracji systemów OT. To kluczowy element planu ciągłości działania, który umożliwi szybkie przywrócenie sprawności po incydencie, np. ataku ransomware. Usługi profesjonalne (U18, U09). Skuteczność wdrożonych rozwiązań zależy od fachowej realizacji. Te usługi zapewnią, że cała infrastruktura zostanie poprawnie skonfigurowana, a niezbędna dokumentacja będzie aktualna i rzetelna. Audyty (U02, U25, U37) i inwentaryzacja OT (U33). Niezależne audyty przeprowadzone na początku i na końcu projektu, wraz z szczegółową inwentaryzacją, pozwolą na dokładną ocenę stanu bezpieczeństwa i zweryfikowanie skuteczności wdrożonych rozwiązań. Szkolenia (U28). Praktyczne, sześciogodzinne szkolenia stanowiskowe oraz z zakresu cyberbezpieczeństwa OT zapewnią personelowi technicznemu niezbędne umiejętności do obsługi i zarządzania nowymi systemami, co jest kluczowe dla ich efektywnego wykorzystania. Data rozpoczęcia projektu: 23.09.2025 Data zakończenia projektu: 30.06.2026
Wydatki rzeczywiście ponoszone	Tak