Cyberbezpieczne Wodociągi

Krajowy Plan Odbudowy i Zwiększania Odporności (inwestycja C3.1.1)

Warszawa, 23.07.2025 roku

LEYTON POLAND

LEYTON
Empower your future

AGENDA

01 Kto może ubiegać się o dofinansowanie

02 Podstawowe informacje o naborze

03 Obszary wsparcia

04 Koszty kwalifikowalne i niekwalifikowalne

05 Przygotowanie i Ocena Wniosków

LEYTON
Empower your future

01 Kto może ubiegać się o dofinansowanie

Kto może ubiegać się o dofinansowanie?

Wsparcie może zostać udzielone podmiotowi prowadzącemu działalność w zakresie zbiorowego zaopatrzenia w wodę, objętemu krajowym system cyberbezpieczeństwa, wykorzystującemu technologie operacyjne w przemysłowych systemach sterowania, który jest:

- przedsiębiorstwem wodociągowo-kanalizacyjnym, które jest operatorem usług kluczowych w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), lub

- spółką prawa handlowego wykonującą zadania o charakterze użyteczności publicznej w rozumieniu przepisów ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), lub

- jednostką sektora finansów publicznych w rozumieniu art. 9 pkt 2–4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756, i 1907 oraz z 2025 r. poz. 39) – (jednostki samorządu terytorialnego oraz ich związki, samorządowe zakłady budżetowe)

LEYTON
Empower your future

02 Podstawowe informacje o naborze

Cyberbezpieczne Wodociągi

Podstawowe informacje (1 z 2)

01 **Cel:**

Wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę, objętych KSC, wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS) w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa

02 **Alokacja środków:**

- 300 mln zł
- Docelowy poziom wskaźnika obowiązującego dla Inwestycji C.3.1.1: objęcie wsparciem 500 podmiotów KSC.

03 **Dofinansowanie:**

- Maksymalna wysokość dofinansowania: 300 tys Euro (pomoc de minimis)
- Poziom dofinasowania: 100% kosztów kwalifikowalnych

Cyberbezpieczne Wodociągi

Podstawowe informacje (2 z 2)

04 Na co?

- wdrożenie środków organizacyjnych służących zapewnieniu cyberbezpieczeństwa (procedury i audyty)
- zakup lub modernizację środków technicznych służących zapewnieniu cyberbezpieczeństwa (sprzęt i usługi –IT i OT)
- rozwój kompetencji personelu w zakresie cyberbezpieczeństwa (szkolenia)

05 Okres kwalifikowalności:

- Przewidywany okres kwalifikowalności wydatków w ramach wsparcia obejmie okres od 1 stycznia 2025 r. do 30 czerwca 2026 r;

06 Gdzie i kiedy składamy wniosek?

- Planowane ogłoszenie naboru: sierpień 2025
- Nabór wniosków potrwa min. 30 dni.
- Operator: Centrum Projektów Polska Cyfrowa (trwa wybór)

LEYTON
Empower your future

03 Obszary wsparcia

Obszary wsparcia

Organizacyjny

wszelkie aspekty organizacyjne bezpieczeństwa systemów teleinformatycznych IT i OT, tj. audyt bezpieczeństwa, audyt zgodności z przepisami i normami, opracowanie, wdrożenie, utrzymanie i aktualizacja systemu zarządzania bezpieczeństwem informacji, systemu zarządzania bezpieczeństwem systemu teleinformatycznego IT/OT, systemu zarządzania ciągłością działania systemu teleinformatycznego IT/OT;

Kompetencyjny

wszelkie działania podnoszące świadomość, wiedzę i umiejętności na poziomie podstawowym, kierowniczym i specjalistycznym w zakresie cyberbezpieczeństwa, realizowane dla pracowników podmiotu, operatorów i administratorów systemów teleinformatycznych IT/OT, kadry kierowniczej IT/OT, kadry kierowniczej i zarządzającej podmiotu;

Techniczny IT

dotyczy obszaru funkcjonalnego IT, obejmuje wszelkie komputerowe środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa komponentów środowiska teleinformatycznego IT, tj.: stacje robocze, serwery, dane biznesowe, oprogramowanie biznesowe, systemy pamięci masowej, urządzenia sieciowe i środowisko sieciowe, systemy bezpieczeństwa fizycznego i technicznego działające w sieci;

Techniczny OT

obejmuje wszelkie komputerowe środki techniczne i wybrane elektrotechniczne środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa komponentów środowiska teleinformatycznego OT/ICS/IoT i środowiska IT obszaru przemysłowego OT, tj.: stacje robocze, serwery, dane systemów OT, systemy OT, oprogramowanie OT, urządzenia sieciowe i środowisko sieciowe OT, systemy bezpieczeństwa wizyjnego, fizycznego i technicznego w ramach infrastruktury wodociągowej (np. stacji uzdatniania wody, punktów poboru wody itp.) działające w sieci;

LEYTON
Empower your future

04 Koszty kwalifikowalne i niekwalifikowalne

Koszty kwalifikowalne

- **środki trwałe/dostawy** (np. sprzęt informatyczny i urządzenia bezpieczeństwa)

- **wartości niematerialne i prawne**, w szczególności autorskie prawa majątkowe lub licencje, w tym subskrypcyjne, na korzystanie z oprogramowania, w tym systemowego o przewidywanym okresie używania dłuższym niż rok, prawa do dokumentacji, raportów i opracowań

- **usługi zewnętrzne**, w szczególności merytoryczne przygotowanie projektu grantowego przez osoby lub podmioty zewnętrzne, usługi informatyczne i szkolenia zwiększające poziom bezpieczeństwa informacji, usługi wspomagające realizację projektu grantowego, w szczególności usługi doradcze osób lub podmiotów zewnętrznych oraz szkolenia, audyty oraz wdrożenie zarządzania bezpieczeństwem i ciągłością działania systemów teleinformatycznych IT/OT

Koszty kwalifikowalne

Cd ..

Łącznie do 20% wydatków kwalifikowalnych projektu grantowego może zostać poniesione na wydatki które mają wpływ na **zapewnienie ciągłości działania systemów teleinformatycznych OT** np.:

• Zasilanie awaryjne: generatory prądu i ups do serwerów, baterie do ups.

• Zabezpieczenie systemów bezpieczeństwa: wizyjnego, dostępu fizycznego i zabezpieczeń technicznych infrastruktury wodociągowej np. stacji uzdatniania wody, punktów poboru wody - działających w sieci rozległej

- **koszty pośrednie** (kwota ryczałtowa do 5% wartości grantu), w szczególności możliwość rozliczenia m.in. kosztów administracyjnych, delegacji, wynagrodzenia kadry zarządzającej projektem grantowym oraz wynagrodzeń osób (umów o pracę) zatrudnionych u grantobiorcy i bezpośrednio zaangażowanych w projekt grantowy (m.in. inżynier kontraktu, ekspert z dziedziny cyberbezpieczeństwa)

Koszty niekwalifikowalne

W szczególności wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa, w szczególności:

- komputery stacjonarne i przenośne, urządzenia mobilne (smartfony, tablety)
- akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki)
- oprogramowanie biurowe, oprogramowanie do elektronicznego zarządzania dokumentacją i oprogramowanie systemów operacyjnych
- szkolenia niezwiązane z cyberbezpieczeństwem
- usługi dostępu do internetu, abonamenty telefoniczne
- budowa infrastruktury sieci LAN/WAN/radiowej/światłowodowej
- budowa infrastruktury systemów bezpieczeństwa: wizyjnego, dostępu fizycznego i zabezpieczeń technicznych
- **podatek VAT oraz wynagrodzenia pracowników jako koszty bezpośrednie**

LEYTON
Empower your future

05 Przygotowanie i Ocena Wniosków

Załączniki obowiązkowe:

- Oświadczenie o nieotrzymaniu **pomocy de minimis** lub zaświadczenia o otrzymanej pomocy de minimis (SKAN) (potwierdzenie wykorzystanego limitu pomocy 300 tys.euro)
- Formularz informacji przedstawianych przy ubieganiu się o **pomoc de minimis** (art. 37 ust. 1 pkt 2 ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej)
- **Zezwolenie na prowadzenie zbiorowego zaopatrzenia w wodę**, o którym mowa w art. 16 ust. 1 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, albo oświadczenie, że podmiot prowadzący działalność w zakresie zbiorowego zaopatrzenia w wodę, objęty krajowym system cyberbezpieczeństwa, przedsiębiorstwo wodociągowo-kanalizacyjne jest podmiotem, o którym mowa w art. 16 ust. 3 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu
- **Oświadczenie** o zapoznaniu się i deklaracja implementacji wytycznych Komunikatu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT)

Ocena Wniosków

ETAPY OCENY

Ocena formalna (0/1):

- Kwalifikowalność Wnioskodawcy
- Niepodleganie wykluczeniu z możliwości otrzymania finansowania ze środków UE
- Wysokość wnioskowanej kwoty
- Okres realizacji projektu
- Zapewnienie zachowania efektów długoterminowych
- Zgodność z celem Projektu
- Zgodność z zasadami horyzontalnymi

Ocena merytoryczna:

- Kwalifikowalność wydatków (0/1)
- Zasadność kosztów w projekcie grantowym (0/1)
- Opis koncepcji projektu grantowego (0/1)
- Ocena planowanego zakresu postępu projektu grantowego (0 - brak rozwiązania, 1 – niski, 2 – średni, 3 - wysoki)

Działania premiowane

Podnoszące w największym stopniu odporność na cyberzagrożenia. W szczególności rozwiązania w których wykorzystywane są technologie operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS). Premia oznacza przyznanie dodatkowych punktów (bonus) za wzrost odporności w premiowanych rozwiązaniach bezpieczeństwa.

Obszar kompetencyjny:

2.1. Szkolenia z zakresu cyberbezpieczeństwa

Obszar techniczny IT:

3.4 Rozwiązanie bezpieczeństwa sieci

3.5 Rozwiązania bezpieczeństwa styku sieci internet z usługami wewnętrznymi

3.12 Monitorowanie bezpieczeństwa

3.14 Zarządzanie uprawnieniami użytkowników

3.15 Zabezpieczanie dowodów cyfrowych

Działania premiowane

Cd ..

Obszar Techniczny OT:

4.1 Bezpieczeństwo systemów sterowania przemysłowego (OT/ICS/IIoT)

4.2 Bezpieczeństwo stacji roboczych OT/ICS

4.3. Rozwiązania bezpieczeństwa sieci OT/ICS/IIoT

4.4 Rozwiązania sieciowe WAN/LAN/WiFi OT/ICS/IIoT

4.5 Rozwiązania bezpieczeństwa styku sieci internet z siecią OT/ICS/IIoT

4.6 Rozwiązania bezpieczeństwa styku sieci wewnętrznej IT z siecią OT/ICS/IIoT

4.7 Rozwiązania kopii zapasowych konfiguracji i danych systemów OT/ICS/IIoT

4.8 Redundancja (HA) OT/ICS/IIoT

4.9 Rozwiązania zarządzania operacyjnego infrastrukturą OT/ICS/IIoT

4.10 Monitorowanie bezpieczeństwa OT/ICS/IIoT

4.11 Reagowanie w zakresie bezpieczeństwa OT/ICS/IIoT

4.12 Wsparcie ciągłości działania infrastruktury obszaru OT (techn. IT/OT/ICS/IIoT)(wydatki limitowane 20%)

Ramowy harmonogram

Etapy konkursu grantowego Cyberbezpieczne Wodociągi	2025 r.					2026 r.					
	VIII	IX	X	XI	XII	I	II	III	IV	V	VI
Ogłoszenie naboru wniosków do konkursu grantowego											
Nabór wniosków o grant											
Ocena wniosków											
Ogłoszenie listy rankingowej wniosków objętych wsparciem											
Zawieranie umów z grantobiorcami											
Przekazanie środków grantobiorcom (jedna transza)											
Realizacja projektów grantowych (**kwalifikowalność wydatków od 1.01.2025 r. do 30.06.2026 r.**)											
Złożenie wniosku rozliczającego (**do 30.06.2026 r.**)											

LEYTON
Empower your future

WARSZAWA

LEYTON Poland Sp. z o.o.
Ul. Wspólna 70
00-687 Warszawa

KRAKÓW

Ul. Pawia 9
31-154 Kraków

POZNAŃ

Ul. Zwierzyniecka 3
60-813 Poznań

TOMASZ WYPYCH

Grants Consultant
twypych@leyton.com
+48 880 575 625

LEYTON.COM