SCHEMAT GRANTOWY - CYBERBEZPIECZNY SAMORZĄD

CEL DOKUMENTU

Niniejszy dokument ma charakter informacyjny i porządkujący oraz określa minimalny zakres procedur udzielania Grantów przez Beneficjenta projektu grantowego.

Konkurs Grantowy pn. „**Cyberbezpieczny Samorząd**" o numerze FERC.02.02-IP.01-0001/23, jest realizowany w ramach Projektu Grantowego w rozumieniu art. 41 ust. 2 ustawy wdrożeniowej[1] przez Beneficjenta, w ramach którego udzielane są Granty na realizację zadań służących osiągnięciu celu Projektu Grantowego.

WYBÓR WNIOSKÓW O PRZYZNANIE GRANTÓW

RAMOWE KRYTERIA WYBORU GRANTOBIORCÓW

Wnioskodawca o przyznanie grantu musi spełniać wszystkie kryteria formalno-merytoryczne, aby jego Wniosek o przyznanie grantu został oceniony pozytywnie. Ocena Wniosku zostanie przeprowadzona w oparciu o kartę oceny formalno-merytorycznej.

Lp.	Nazwa kryterium	Opis kryterium	Punktacja
1	Kwalifikowalność Wnioskodawcy	Weryfikacji podlega czy Wnioskodawca grantowy jest jednostką samorządu terytorialnego, zgodnie z załącznikiem nr	0-1

[1] Ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (t.j. Dz. U. z 2025 r. poz. 1733, z późn. zm.), dalej „ustawa wdrożeniowa".

Lp.	Nazwa kryterium	Opis kryterium	Punktacja
		2 do Regulaminu Konkursu oraz czy Wniosek został złożony w trakcie prowadzonego naboru.	
2	Niepodleganie wykluczeniu z możliwości otrzymania finansowania ze środków Unii Europejskiej	Weryfikacji podlega czy Wnioskodawca grantowy nie został wykluczony z możliwości otrzymania finansowania ze środków UE - kryterium weryfikowane na podstawie oświadczeń zawartych we Wniosku o przyznanie grantu.	0-1
3	Wysokość wnioskowanej kwoty	Weryfikacji podlega czy wnioskowana kwota nie przekracza maksymalnej kwoty wskazanej w Regulaminie Konkursu zgodnie z załącznikiem nr 2.	0-1
4	Okres realizacji Projektu	Okres realizacji Projektu nie przekracza terminu wskazanego w Regulaminie Konkursu.	0-1
5	Kwalifikowalność wydatków	Weryfikacji podlega czy wskazane we Wniosku wydatki są kwalifikowalne i zgodne z Regulaminem Konkursu Grantowego.	0-1
6	Zasadność kosztów w Projekcie	Weryfikacji podlega czy Wnioskodawca grantowy wystarczająco uzasadnił	0-1

Lp.	Nazwa kryterium	Opis kryterium	Punktacja
		potrzebę wskazanych wydatków oraz ich racjonalność w kontekście celu Projektu oraz potrzeb Wnioskodawcy.	
7	Zapewnienie utrzymania efektów Projektu	Weryfikacji podlega czy efekty Projektu zostaną utrzymane przez min. 2 lata od zakończenia Projektu. Ocena na podstawie oświadczenia Wnioskodawcy grantowego o zapoznaniu się z Regulaminem Konkursu Grantowego i akceptacji jego zasad, zawartych we Wniosku o przyznanie grantu.	0-1
8	Opis koncepcji Projektu	Weryfikacji podlega, czy Wnioskodawca grantowy przedstawił opis koncepcji Projektu zawierający informacje o: • potrzebach Wnioskodawcy grantowego w zakresie cyfryzacji urzędu w tym zwiększenia poziomu bezpieczeństwa informacji urzędu, a także jednostek podległych (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia) - jeśli dotyczy; • celach i efektach Projektu, w tym	0-1

Lp.	Nazwa kryterium	Opis kryterium	Punktacja
		w odniesieniu do celów Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2; • zapewnieniu zgodności Projektu z zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami; równości kobiet i mężczyzn.	

ZASADY I SPOSÓB WYBORU GRANTOBIORCÓW W OTWARTYM NABORZE Z ZACHOWANIEM ZASADY BEZSTRONNOŚCI I PRZEJRZYSTOŚCI

Nabór Wniosków

Informacja o naborze wniosków, zasady Konkursu i link do aplikacji służącej do składania wniosków zostaną opublikowane na stronie CPPC - Cyberbezpieczny Samorząd.

Nabór Wniosków w ramach otwartego Konkursu Grantowego

Nabór Wniosków odbędzie się w ramach otwartego naboru grantowego, ogłaszanego na stronie Cyberbezpieczny Samorząd. Nabór skierowany będzie do Jednostek Samorządu Terytorialnego wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia).

Nabór potrwa od 19.07.2023 r. do 14.12.2023 r. (do godziny 16:00)

Przewidywana liczba Grantów i alokacja

1. Alokacja na Granty w Konkursie Grantowym pn. “Cyberbezpieczny Samorząd” wynosi 1 762 235 453,00 PLN (w tym środki unijne w wysokości 1 465 303 702,00

PLN i środki z budżetu państwa w wysokości 296 931 751,00 PLN).

2. Maksymalna wysokość przyznanego Grantu dla Projektu może wynosić do 100% kosztów kwalifikowalnych.

3. Minimalna wysokość Grantu dla jednego Grantobiorcy wynosi 200 000 PLN, natomiast maksymalna wysokość Grantu wynosi 850 000 PLN. W przypadku powiatów i województw wysokość grantu wynosi 850 000 PLN. Wysokość wkładu własnego zależna jest od współczynnika zamożności danego JST.

4. Wysokość przyznanego Grantu dla poszczególnych JST może zostać zwiększona powyżej wartości określonej w § 4 ust. 4 Regulaminu Konkursu Grantowego i ogłoszona przez Beneficjenta w przypadku ewentualnego naboru uzupełniającego określonego zgodnie z § 5 ust. 1 pkt. 2 Regulaminu Konkursu Grantowego.

5. Przewidywana liczba Wniosków o przyznanie grantu to co najmniej 1935, a maksymalnie 2807.

Sposób składania Wniosków

Wnioski składane są w formie elektronicznej za pośrednictwem LSI - aplikacji do składania Wniosków dostępnej na stronie Cyberbezpieczny Samorząd oraz LSI - Beneficjent.

Sposób i zasady oceny Wniosków

Ocena Wniosków będzie dokonywana przez Komisję Przyznającą Granty (KPG). Po wstępnej walidacji Wniosku o przyznanie grantu możliwe będzie naniesienie poprawek przez Grantobiorcę zgodnie z uwagami KPG. Szczegółowe zasady oceny Wniosków znajdują się w Regulaminie Konkursu Grantowego.

Wydatki kwalifikowalne i sposób rozliczania Grantów

1. Do wydatków kwalifikowanych w ramach Grantu zalicza się w szczególności:

1) Środki trwałe/Dostawy:
   a) Sprzęt informatyczny i Urządzenia bezpieczeństwa:
      - Firewall sieciowy;
      - WAF (Web Application Firewall);
      - SIEM (Security Information and Event Management);
      - UTM (Unified Threat Management);
      - IPS (Intrusion Prevention System);
      - IDS (Intrusion Detection System);
      - VPN (Virtual Private Network);
      - NAC (Network Access Control);
      - proxy sprzętowe;
      - serwer;
      - serwer do wykonywania kopii zapasowych;
      - macierz dyskowa;
      - dyski twarde do macierzy dyskowej;
      - Network Attached Storage (NAS);
      - Storage Area Network (SAN);
      - Web Secure Gateway;
      - Email Secure Gateway;
      - generator prądu;
      - UPS;
      - ochrona AntyDDoS;
      - zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X;

2) wartości niematerialne i prawne, w szczególności:
   a) wartości niematerialne i prawne, takie jak: 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, opracowań. Koszty są kwalifikowalne w okresie określonym w Umowie o powierzenie grantu, zgodnie z zasadami wskazanymi w § 3 ust. 11 pkt 1-3 Regulaminu Konkursu Grantowego:
      - oprogramowanie antywirusowe;
      - oprogramowanie typu EDR (Endpoint Detection and Response);

- oprogramowanie typu XDR (Extended Detection and Response);
- oprogramowanie do wykonywania kopii zapasowych;
- oprogramowanie antyspamowe;
- oprogramowanie WAF (Web Application Firewall);
- oprogramowanie SIEM (Security Information and Event Management);
- oprogramowanie Menadżera logów;
- oprogramowanie do zarządzania podatnościami;
- programowanie przeciwdziałającemu wyciekowi danych (DLP – Data Leak Prevention);
- oprogramowanie do zarządzania uprzywilejowanemu dostępowi (PAM-Privileged Access Management);
- oprogramowanie Web Secure Gateway;
- oprogramowanie Email Secure Gateway;
- oprogramowanie do zarządzania tożsamością i dostępem;
- oprogramowanie centralnego menadżera haseł;
- oprogramowanie do monitorowania infrastruktury informatycznej;
- oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych;
- oprogramowanie do badania podatności systemów informatycznych;
- oprogramowanie do badania podatności serwisów WWW;
- oprogramowanie do badania podatności w kodzie aplikacji;
- oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików;
- oprogramowanie do analizy po włamaniowej;
- oprogramowanie do ochrony przed ransomware;

3) usługi zewnętrzne - kwalifikowane wyłącznie w okresie realizacji Projektu, w szczególności:

a) przygotowanie Projektu: sfinansowanie przygotowania Projektu opracowanego przez specjalistów / organizacje, w których osoba odpowiedzialna za przygotowania Projektu posiada stosowną wiedzę i

m.in. 2 letnie doświadczenie we wnioskowanym zakresie oraz co najmniej 1 (jeden) certyfikat świadczący o posiadanej wiedzy w danym zakresie.;

b) usługi informatyczne. Pokrycie kosztów zwiększających poziom bezpieczeństwa informacji, tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych:
   - usługa poczty elektronicznej w chmurze obliczeniowej typu IaaS, SaaS, PaaS z elementami bezpieczeństwa;
   - usługa testowania bezpieczeństwa infrastruktury sieciowej;
   - usługa testowania bezpieczeństwa serwisów internetowych;
   - usługa testowania bezpieczeństwa aplikacji;
   - usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS w zakresie sandbox do badania bezpieczeństwa aplikacji oraz plików;
   - usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego;

c) usługi wspomagające realizację Projektu, w szczególności usługi doradcze podmiotów posiadających stosowne kwalifikacje i min. 2 letnim doświadczeniem w prowadzeniu projektów z obszaru cyberbezpieczeństwa oraz stosowne certyfikaty lub równoważne poświadczenia (np. Kwalifikację zawodową) potwierdzające możliwość wykonania zlecenia;

d) szkolenia: zakup i organizacja szkoleń stacjonarnych lub/ i online dedykowanych dla pracowników JST zorganizowanych przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.;

e) informacja i promocja: pokrycie kosztów przygotowania i wyprodukowania (drukowanych i elektronicznych) materiałów promocyjnych i informacyjnych upowszechniających świadomość o zagrożeniach cybernetycznych, np.: sfinansowanie przygotowania newslettera dla pracowników; przygotowanie periodyku o cyberhigienie dla pracowników; materiałów

budujących i wzmacniających świadomość o zagrożeniach cybernetycznych.

2. Do wydatków niekwalifikowalnych w ramach Projektu zaliczają się:

1) do współfinansowania nie kwalifikują się wszelkie wydatki określone w podrozdziale 3.4. Katalogu wydatków kwalifikowanych II i IV priorytetu programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027;

2) do współfinansowania nie kwalifikują się wszelkie wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa w JST, w szczególności:
   a) komputery stacjonarne i przenośne;
   b) urządzenia mobilne tj. smartfony lub tablety;
   c) akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, klawiatury, myszy);
   d) materiały eksploatacyjne;
   e) oprogramowanie biurowe, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;
   f) szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;
   g) usługi dostępu do Internetu, abonamenty telefoniczne.

3. JST będą zobowiązane do przeprowadzenia Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 6 do Regulaminu Konkursu Grantowego w następujących terminach:

   a. do 30 dni od podpisania Umowy o udzielenie grantu;
   b. wraz z Wnioskiem rozliczającym Grant.

4. Uzupełniona Ankieta przekazywana jest do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP na adres skrytki: /NASK- Instytut/SkrytkaESP (akronim/temat: **cyberbezpieczny.samorzad.ankieta**).

W celu rozliczenia Grantu, Grantobiorca składa Operatorowi Wniosek rozliczający, do którego załącza dokumentację finansową potwierdzająca poniesienie wydatków (w tym faktury lub równoważne dowody księgowe wraz z potwierdzeniem dowodów zapłaty), protokół/protokoły odbioru

sprzętu/oprogramowania/usługi, z wyszczególnionymi ilościami i specyfikacją zakupionego sprzętu/oprogramowania/usług oraz listę podmiotów, którym przekazano sprzęt/oprogramowanie/usługę. Na potwierdzenie ubezpieczenia sprzętu zostanie przedstawiona polisa obejmująca zadeklarowany sprzęt.
W zakresie potwierdzenia prawidłowości wyboru przez Grantobiorcę

dostawców i wykonawców - na żądanie CPPC lub Operatora - Grantobiorca przedłoży dokumentację z postępowania o udzielenie zamówienia przeprowadzonego zgodnie z Wytycznymi Ministra Funduszy i Polityki Regionalnej dotyczącymi kwalifikowalności wydatków na lata 2021-2027 lub ustawą z dnia 11 września 2019 r - Prawo zamówień publicznych.

5. Warunkiem zakwalifikowania wydatków na sprzęt informatyczny jest zakup nowego sprzętu IT.

6. Okres realizacji Projektu został określony w § 3 ust. 10 pkt 1 Regulaminu Konkursu Grantowego.

7. Grantobiorca i Grantodawca mogą w Umowie o powierzenie grantu uzgodnić krótszy okres realizacji Projektu, zgodnie z zapisami § 3 ust. 10 pkt 2 Regulaminu Konkursu Grantowego.

8. W ramach Projektu kwalifikowalne są wydatki poniesione zgodnie z § 3 ust. 11 pkt 1 Regulaminu Konkursu Grantowego.

9. Grantodawca i Grantobiorca mogą w Umowie o powierzenie grantu uzgodnić krótszy okres kwalifikowalności wydatków w Projekcie, o ile wynika to z postanowień Umowy o powierzeniu grantu. W przypadku uzgodnienia przez Grantobiorcę i Grantodawcę krótszego okresu realizacji Projektu, zgodnie z § 3

ust. 11 pkt 2 Regulaminu Konkursu Grantowego, okres kwalifikowalności wydatków trwa od **1.06.2023 r.** i kończy się wraz z końcem okresu realizacji Projektu uzgodnionym przez Grantobiorcę i Grantodawcę w Umowie o powierzenie grantu.

10. Jeżeli wydatek (w szczególności na wartości niematerialne i prawne) obejmuje okres wykraczający poza okres kwalifikowalności wydatków określony odpowiednio zgodnie z § 3 ust. 11 pkt 1 lub 2 Regulaminu Konkursu Grantowego, będzie on kwalifikowalny wyłącznie w części proporcjonalnej do okresu kwalifikowalności wydatków, zgodnie z § 3 ust. 11 pkt 3 Regulaminu Konkursu Grantowego.

11. Grantobiorca jest zobowiązany do wydatkowania Grantu zgodnie z przepisami obowiązującego prawa, w sposób oszczędny, racjonalny i efektywny w okresie realizacji Projektu i zgodnie z jego celami.

12. Grantobiorca dokonując zakupu środków trwałych, wartości niematerialnych i prawnych oraz usług wskazanych jako kwalifikowane w ramach Projektu o wartości równej lub niższej niż kwota określona w art. 2 ust 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, a jednocześnie przekraczającej 50 tys. zł netto, tj. bez podatku od towarów i usług (VAT), jest zobligowany do stosowania bazy konkurencyjności dostępnej pod adresem Baza konkurencyjności, zgodnie z Wytycznymi dotyczącymi kwalifikowalności wydatków oraz postanowieniami Umowy o powierzenie grantu.

13. Grantobiorca jest zobowiązany do utrzymania efektów Projektu, w tym do opracowania oraz wdrożenia procedury monitorowania utrzymania efektów Projektu, zgodnie z postanowieniami Umowy o powierzenie grantu. Obejmuje to w szczególności: tj.: utrzymania środków trwałych i usług nabytych w ramach Projektu przez okres 2 lat od dnia zakończenia Projektu.

14. Za zakończenie Projektu rozumie się moment akceptacji przez Operatora końcowego rozliczenia Grantu po spełnieniu przez Grantobiorcę warunków, o których mowa w § 3 ust. 2 Umowy o powierzenie grantu.

Zasady dotyczące monitorowania i kontroli Projektów

Operator przygotuje plan kontroli i wskaże listę Grantobiorców, w przypadku których dokona kontroli.

Możliwe formy kontroli to: kontrola zza biurka (pogłębiona weryfikacja w oparciu o dokumentację) oraz kontrola na miejscu realizacji Projektu.

Zasady dotyczące odzyskiwania Grantów w przypadku ich wykorzystania niezgodnie z celami Projektu lub niewykorzystania

Umowa o powierzenie grantu określa sposób postępowania w przypadku stwierdzenia, że Projekt jest realizowany niezgodnie z umową.

Umowa o powierzenie grantu określa również sposób zwrotu środków w przypadku nie osiągnięcia przez Grantobiorcę wskaźników Projektu na zakładanym poziomie.

Kontakt z Wnioskodawcami:

Wszelkie informacje pozyskają Państwo na stronie Cyberbezpieczny Samorząd.
Kontakt e-mail: **cyberbezpiecznysamorzad@cppc.gov.pl**.
Infolinia obsługiwaną przez Operatora pod nr: **22 182 22 94**.
Odpowiedzi polegające na wyjaśnieniu procedur będą dodatkowo zamieszczane w pytaniach i odpowiedziach.