

## SCHEMAT GRANTOWY

### Cyberbezpieczny Samorząd

#### CEL DOKUMENTU

Niniejszy dokument określa minimalny zakres procedur udzielania grantów przez Beneficjenta projektu grantowego.

Realizacja konkursu pn. „**Cyberbezpieczny Samorząd**”, następuje w formie projektu grantowego w rozumieniu art.41 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (t.j. Dz. U. z 2022 r. poz. 1079), dalej “ustawa wdrożeniowa”.

#### WYBÓR PROJEKTÓW GRANTOWYCH

##### RAMOWE KRYTERIA WYBORU GRANTOBIORCÓW

Wnioskodawca 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 Wnioskodawcą jest jednostką samorządu terytorialnego, zgodnie z załącznikiem nr 2 do Regulaminu konkursu oraz czy wniosek został złożony w trakcie prowadzonego naboru.	0-1
2	Niepodleganie wykluczeniu z możliwości otrzymania dofinansowania ze środków Unii Europejskiej	Weryfikacji podlega czy Wnioskodawca nie został wykluczony z możliwości otrzymania dofinansowania 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 wystarczająco uzasadnił potrzebę wskazanych wydatków oraz ich racjonalność w kontekście celu projektu oraz potrzeb Grantobiorcy.	0-1
7	Zapewnienie utrzymania efektów projektu	Weryfikacji podlega czy efekty projektu zostaną utrzymane przez min. 2 lata od zakończenia projektu.  Ocena na podstawie oświadczenia Wnioskodawcy o zapoznaniu się z regulaminem konkursu i akceptacji jego zasad, zawartych we Wniosku o przyznanie Grantu.	0-1
8	Opis koncepcji projektu	Weryfikacji podlega, czy Wnioskodawca przedstawił opis koncepcji projektu zawierający informacje o: <ul style="list-style-type: none"> <li>- potrzebach Wnioskodawcy 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;</li> <li>- celach i efektach projektu, w tym w odniesieniu do celów Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2;</li> <li>- zapewnieniu zgodności projektu z zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami; równości kobiet i mężczyzn.</li> </ul>	0-1

## ZASADY I SPOSÓB WYBORU GRANTOBIORCÓW W OTWARTYM NABORZE Z ZACHOWANIEM ZASADY BEZSTRONNOŚCI I PRZEJRZYŚCI

### Nabór wniosków

Informacja o naborze wniosków, zasady konkursu i link do aplikacji służącej do składania wniosków zostaną opublikowane na stronie CPPC - [www.gov.pl/cppc/cyberbezpieczny-samorzad](http://www.gov.pl/cppc/cyberbezpieczny-samorzad).

## Nabór wniosków w ramach otwartego konkursu grantowego

Nabór wniosków odbędzie się w ramach otwartego naboru grantowego, ogłaszanego na stronie [www.gov.pl/cppc/cyberbezpieczny-samorzad](http://www.gov.pl/cppc/cyberbezpieczny-samorzad). 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 30.11.2023 r. (do godziny 16:00)**

### Przewidywana liczba grantów i alokacja

1. Alokacja na Granty w konkursie „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 intensywność dofinansowania projektu grantowego „Cyberbezpieczny Samorząd” 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 dofinansowania w ramach Grantów 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 grantowych 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 [www.gov.pl/cppc/cyberbezpieczny-samorzad](http://www.gov.pl/cppc/cyberbezpieczny-samorzad) oraz <https://lsi.cppc.gov.pl/beneficjent>

### Sposób i zasady oceny wniosków

Ocena będzie dokonywana przez Komisję Przyznającą Granty (KPG). Po wstępnej walidacji wniosku grantowego 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:

L.p.	Nazwa produktu
------	----------------

L.p.	Nazwa produktu
1	Firewall sieciowy
2	WAF (Web Application Firewall)
3	SIEM (Security Information and Event Management)
4	UTM (Unified Threat Management)
5	IPS (Intrusion Prevention System)
6	IDS (Intrusion Detection System)
7	VPN (Virtual Private Network)
8	NAC (Network Access Control)
9	Proxy sprzętowe
10	Serwer
11	Serwer do wykonywania kopii zapasowych
12	Macierz dyskowa
13	Dyski twarde do macierzy dyskowej
14	Network Attached Storage (NAS)
15	Storage Area Network (SAN)
16	Web Secure Gateway
17	Email Secure Gateway
18	Generator prądu
19	UPS
20	Ochrona AntyDDoS
21	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 kwalifikowane będą tylko w okresie realizacji projektu.

L.p.	Nazwa produktu
1	Oprogramowanie antywirusowe
2	Oprogramowanie typu EDR (Endpoint Detection and Response)
3	Oprogramowanie typu XDR (Extended Detection and Response)
4	Oprogramowanie do wykonywania kopii zapasowych
5	Oprogramowanie antyspamowe
6	Oprogramowanie WAF (Web Application Firewall)
7	Oprogramowanie SIEM (Security Information and Event Management)

8	Oprogramowanie Menadżera logów
9	Oprogramowanie do zarządzania podatnościami
10	Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention)
11	Oprogramowanie do zarządzania uprzywilejowanym dostępowi (PAM- Privileged Access Management)
12	Oprogramowanie Web Secure Gateway
13	Oprogramowanie Email Secure Gateway
14	Oprogramowanie do zarządzania tożsamością i dostępem
15	Oprogramowanie centralnego menadżera haseł
16	Oprogramowanie do monitorowania infrastruktury informatycznej
17	Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych
18	Oprogramowanie do badania podatności systemów informatycznych
19	Oprogramowanie do badania podatności serwisów WWW
20	Oprogramowanie do badania podatności w kodzie aplikacji
21	Oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików
22	Oprogramowanie do analizy powłamaniowej
23	Oprogramowanie do ochrony przed ransomware

3) Usługi zewnętrzne, 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. Koszty będą kwalifikowane tylko w okresie realizacji projektu.
- b) Usługi informatyczne. Pokrycie kosztów zwiększających poziom bezpieczeństwa informacji, tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych tylko w okresie realizacji projektu:

L.p.	
1	Usługa poczty elektronicznej w chmurze obliczeniowej typu IaaS, SaaS, PaaS z elementami bezpieczeństwa
2	Usługa testowania bezpieczeństwa infrastruktury sieciowej
3	Usługa testowania bezpieczeństwa serwisów internetowych
4	Usługa testowania bezpieczeństwa aplikacji
5	Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS w zakresie sandbox do badania bezpieczeństwa aplikacji oraz plików
6	Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego

- c) Usługi wspomagające realizację projektu, w szczególności usługi doradcze świadczone przez podmioty posiadające stosowne kwalifikacje i m.in. 2 letnie doświadczenie w prowadzeniu projektów z obszaru cyberbezpieczeństwa oraz stosowne certyfikaty lub równoważne poświadczenia (np. Kwalifikację zawodową) potwierdzające możliwość wykonania zlecenia. Kwalifikowalność kosztów tylko w okresie realizacji projektu.
  - d) Szkolenia. Zakup i organizacja szkoleń stacjonarnych lub/ i online dedykowanych dla pracowników JST zorganizowanych przez podmioty posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. Kwalifikowalność kosztów tylko w okresie realizacji projektu.
  - 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 Grantu zaliczają się:
- 1) Do współfinansowania nie kwalifikują się wszelkie wydatki określone w podrozdziale 3.3. Katalogu wydatków kwalifikowanych II 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 dokumentacji konkursowej 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 potwierdzającą poniesienie wydatków (w tym faktur lub równoważnych dowodów księgowych 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 w ubezpieczeniu sprzęt. W zakresie potwierdzenia prawidłowości wyboru dostawców i wykonawców - na żądanie CPPC lub Operatora, Grantobiorca przedłoży dokumentację z postępowania o udzielenie zamówienia, zgodnie z Wytocznymi 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. W ramach grantu kwalifikowalne są wydatki na sprzęt zakupiony od 01.06.2023 r. do końca realizacji projektu grantowego, zgodnie z Umową o powierzenie grantu.
7. Projekt grantowy powinien trwać maksymalnie **24 miesiące** od dnia wejścia w życie Umowy o powierzenie Grantu, jednak nie później niż do **30.06.2026 r.**;
8. 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.
9. 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 <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>.
10. Grantobiorca jest zobowiązany do utrzymania efektów projektu grantowego, w tym do opracowania oraz wdrożenia procedury monitorowania utrzymania efektów projektu tj. utrzymania środków trwałych i usług nabytych w ramach projektu przez okres 2 lat od dnia zakończenia projektu oraz utrzymania trwałości projektu grantowego (jeśli dotyczy). Za zakończenie projektu grantowego rozumie się zaakceptowanie przez Operatora końcowego rozliczenia projektu grantowego.

### **Zasady dotyczące monitorowania i kontroli grantów**

Operator przygotowuje 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 grantowego 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 wskaźników na zakładanym poziomie.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

Dofinansowane przez  
Unię Europejską



### **Kontakt z Wnioskodawcami:**

Wszelkie informacje pozyskają Państwo na stronie [www.gov.pl/cppc/cyberbezpieczny-samorzad](http://www.gov.pl/cppc/cyberbezpieczny-samorzad),  
kontakt e-mail: [cyberbezpiecznysamorzad@cppc.gov.pl](mailto:cyberbezpiecznysamorzad@cppc.gov.pl) oraz na infolinię obsługiwaną przez  
Operatora pod nr: 22 182 22 94. Odpowiedzi polegające na wyjaśnieniu procedur będą dodatkowo  
zamieszczane w pytaniach i odpowiedziach.