Regulamin Konkursu Grantowego

Cyberbezpieczny Samorząd

Priorytet II: Zaawansowane usługi cyfrowe

Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Warszawa, sierpień 2023 r.

§1

Słownik pojęć

Ankieta - „Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", opracowana przez Operatora, na potrzeby oceny poziomu dojrzałości cyberbezpieczeństwa u Grantobiorcy, dostępna na stronie internetowej konkursu „Cyberbezpieczny Samorząd", wypełniana przez Grantobiorcę po zawarciu Umowy oraz przy składaniu wniosku rozliczającego i każdorazowo przekazywana Operatorowi, stanowiąca załącznik nr 7 do dokumentacji konkursowej.

Beneficjent – Beneficjent projektu Cyberbezpieczny Samorząd - Centrum Projektów Polska Cyfrowa (CPPC);

FERC – Fundusze Europejskie na Rozwój Cyfrowy 2021-2027;

Grant – środki finansowe, które Operator na podstawie Umowy o powierzenie Grantu powierzył Grantobiorcy na realizację zadań służących osiągnięciu celu Projektu;

Grantobiorca – podmiot, będący jednostką samorządu terytorialnego, uprawniony do udziału w konkursie, wybrany w procesie otwartego naboru, ogłoszonego przez Grantodawcę, który realizuje Projekt Grantowy na podstawie Umowy o powierzenie Grantu;

Grantodawca – Grantodawca projektu indykatywnego Cyberbezpieczny Samorząd - Centrum Projektów Polska Cyfrowa (CPPC);

JST – jednostki samorządu terytorialnego uprawnione do wnioskowania o Grant w ramach Konkursu Grantowego;

Komisja Przyznająca Granty (KPG) – komisja zatwierdzająca listę wniosków o przyznanie Grantu według zasad określonych w niniejszym Regulaminie;

Konkurs Grantowy – nabór prowadzony przez Operatora w celu wyłonienia Grantobiorców;

LSI – aplikacja służąca do kompleksowej obsługi wniosków grantowych (w zakresie składania wniosków, oceny wniosków, komunikacji między Operatorem a Wnioskodawcą), dostępna na stronie internetowej Projektu oraz na stronie https://lsi.cppc.gov.pl/beneficjent;

NASK - Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;

Operator – Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;

Partner - Partner Projektu – Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;

Partner Wiodący – Partner wiodący projektu indykatywnego Cyberbezpieczny Samorząd - Centrum Projektów Polska Cyfrowa (CPPC);

Projekt – przedsięwzięcie realizowane przez Centrum Projektów Polska Cyfrowa pod nazwą „Cyberbezpieczny Samorząd";

Projekt Grantowy - projekt realizowany przez Grantobiorcę, na podstawie Umowy o powierzenie Grantu zawartej z CPPC;

Regulamin, Regulamin Konkursu Grantowego – niniejszy Regulamin naboru;

Strona internetowa Projektu - http://www.gov.pl/cppc/cyberbezpieczny-samorzad

SZOP - Szczegółowy Opis Priorytetów Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027;

Umowa o powierzenie Grantu - umowa pomiędzy Grantobiorcą i Grantodawcą określająca w szczególności

przedmiot umowy, zadania Grantobiorcy objęte grantem, kwotę grantu, okres realizacji umowy o powierzenie grantu, warunki przekazania i rozliczenia grantu;

Ustawa wdrożeniowa - ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz.U. 2022 poz. 1079);

Wniosek o przyznanie Grantu, Wniosek – wniosek grantowy (którego wzór stanowi załącznik nr 1) złożony za pośrednictwem aplikacji do składania wniosków, dostępnej na stronie: www.gov.pl/cppc/cyberbezpieczny-samorzad;

Wnioskodawca – podmiot, będący jednostką samorządu terytorialnego, aplikujący o Grant na realizację Projektu Grantowego, który złożył za pomocą LSI Wniosek o przyznanie Grantu;

Wskaźniki projektu – wskaźniki projektu (których wzór stanowi załącznik nr 9 do Regulaminu Konkursu Grantowego).

§2

Podstawy prawne

1. Konkurs Grantowy jest organizowany w oparciu o następujące akty prawne:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z 24.06.2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej (Dz.Urz. UE L 231, s. 159, ze sprost.), zwany dalej „rozporządzeniem ogólnym";

2) Ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079 ze zm.), zwana dalej „ustawą wdrożeniową";

3) Program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, zwany dalej „FERC lub Program", przyjęty decyzją wykonawczą Komisji Europejskiej z dnia 18 listopada 2022 r.;

4) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2021 r. poz. 1797).

5) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913)

§3

Informacje ogólne

1. Celem Konkursu Grantowego jest wybór do dofinansowania projektów, które przyczynią się do osiągnięcia celów FERC oraz celów działania określonych w SZOP. Do celów tych należy w szczególności wsparcie JST w zakresie realizacji usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji jednostek samorządu terytorialnego wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia) w kontekście zwiększenia poziomu cyberbezpieczeństwa.

2. Dofinansowanie udzielane w formie grantów może być przeznaczone na zadania w ramach poniżej wskazanych obszarów:

1.	Obszar organizacyjny	Środki można przeznaczyć na następujące działania (usługi): • opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym między innymi wprowadzenie lub aktualizacja polityk bezpieczeństwa informacji (PBI), na analizy ryzyka (w tym opracowanie i wdrożenie metodyk), np. procedury: obsługi incydentów, ciągłości działania i zarządzania kryzysowego, stosowania kryptografii i szyfrowania, kontroli dostępu, bezpieczeństwa pracy zdalnej, używania urządzeń mobilnych, itp. • audyt SZBI, audyt zgodności KRI/uoKSC przez

		wykwalifikowanych audytorów, (re-)certyfikacja SZBI na zgodność z normami.
2.	Obszar kompetencyjny	Środki można przeznaczyć na następujące działania (usługi): • podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST, • szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji, • szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach projektu grantowego, • szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.
3.	Obszar techniczny	Środki można przeznaczyć na następujące działania (usługi): • zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta, • zakup, wdrożenie i utrzymanie rozwiązań ciągłego monitorowania bezpieczeństwa, skanery podatności, zarządzanie podatnościami, zarządzanie zasobami IT i aktywami podlegającymi ochronie oraz innych rodzajów narzędzi wymienionych poniżej w katalogu klas rozwiązań, • zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa, • zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa, • zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa

		(SOC), także jako element Centrum Usług Wspólnych, • zakup testów i badań bezpieczeństwa, dostępu do informacji bezpieczeństwa (np. ang. feeds) oraz inne usługi integracyjne dotyczące obszaru cyberbezpieczeństwa.

3. Grantobiorca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247), zwanego dalej „rozporządzeniem KRI", zgodnie z poniższymi warunkami:
   1) Zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001;
   2) Raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST i dostarczony do Grantobiorcy;
   3) Niezwłocznie po uzupełnieniu i podpisaniu raportu z audytu, Grantobiorca zobowiązany jest uzupełnić wniosek rozliczający projekt o dodatkowy załącznik nr 6 do Regulaminu Konkursu Grantowego oraz przekazać całość do Operatora za pośrednictwem aplikacji dedykowanej do rozliczeń;
   4) Audyt systemu bezpieczeństwa informacji wdrożonego u Grantobiorcy zostanie przeprowadzony na wniosek Grantobiorcy przez:

a. audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub;

b. audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001;

   5) Przeprowadzenie audytu systemu bezpieczeństwa informacji wdrożonego u Grantobiorcy i przekazanie do Operatora raportu z audytu wraz z załącznikiem nr 6 do Regulaminu Konkursu Grantowego, nastąpi na zakończenie realizacji projektu grantowego (jako załączniki do wniosku rozliczającego projekt).

4. Niniejszy Regulamin określa szczegółowe zasady powierzania Grantów w ramach Konkursu Grantowego.
5. Konkurs Grantowy jest prowadzony na terenie całej Polski.
6. Konkurs Grantowy przeprowadzany jest jawnie, z zapewnieniem publicznego dostępu do informacji o zasadach jego przeprowadzania oraz listy Projektów Grantowych, które otrzymały Grant.
7. Nabór wniosków odbędzie się w ramach otwartego naboru grantowego.
8. Grantobiorcy będą realizowali Projekty Grantowe na podstawie Umowy o powierzenie Grantu, zawartejz Beneficjentem.
9. Warunki dotyczące okresu realizacji Projektu Grantowego:
   1) okres realizacji Projektu Grantowego wynosi maksymalnie **24 miesiące** od dnia wejścia w życie Umowy o powierzenie Grantu, jednak nie później niż do **30.06.2026 r.;**

2) dopuszcza się kwalifikowalność wydatków poniesionych w okresie **od dnia 01.06.2023 r**. do dnia zakończenia realizacji Projektu Grantowego określonego w Umowie o powierzenie Grantu.

10. Wniosek o przyznanie Grantu uznaje się za złożony, jeśli spełnia następujące warunki:

1) został złożony w terminie, o którym mowa w § 5 ust. 1, pkt 3.

2) został złożony zgodnie z zasadami określonymi w § 5 ust. 2.

11. Na podstawie art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913) krajowy system cyberbezpieczeństwa obejmuje jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270 z późn. zm.).

Zgodnie z art. 9 pkt 2 ustawy o finansach publicznych sektor finansów publicznych tworzą jednostki samorządu terytorialnego oraz ich związki. Działalność z zakresu cyberbezpieczeństwa stanowi część zasadniczych funkcji państwa i w związku z tym art. 107 ust. 1 Traktatu o Funkcjonowaniu Unii Europejskiej dotyczący pomocy publicznej nie ma zastosowania, ponieważ w tym zakresie jednostki samorządu terytorialnego działają sprawując władzę publiczną.

Obowiązek zapewnienia bezpieczeństwa publicznego, w tym cyberbezpieczeństwa, wynika również z ustaw ustrojowych każdej jednostki samorządu terytorialnego.

§4

Podmioty uprawnione do udziału w Konkursie grantowym i zasady finansowania projektów

1. Do udziału w Konkursie Grantowym uprawnione są JST wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia) – zgodnie z listą Wnioskodawców publikowaną w dniu ogłoszenia naboru.
2. 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).**
3. Maksymalna intensywność dofinansowania projektu grantowego „Cyberbezpieczny Samorząd" może wynosić do **100%** kosztów kwalifikowalnych.
4. W przypadku gmin 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.
5. Wysokość dofinansowania w ramach Grantów dla poszczególnych JST zostanie określona zgodnie z metodologią opartą o wskaźniki G/P/W „wskaźnik podstawowych dochodów podatkowych na 1 mieszkańca gminy/powiatu/województwaprzyjęty do obliczania subwencji wyrównawczej w 2023 r.", publikowany przez Ministerstwo Finansów, a także liczbę mieszkańców w danej jednostce. Wartość wskaźnika dla kraju w 2023 r. wynosi G = 2246,66, P = 312,20 i W = 412,86. Kwota dofinansowania dla gminy/powiatu/województwa uzależniona jest od stosunku wskaźnika dla danego G/P/W do wskaźnika oszacowanego dla kraju i wyrażona jest następującym wzorem:

GMINY

Metodologia wyliczenia wysokości grantu dla gminy:

Dane wyjściowe:

1. Wysokość grantu w przedziale od 200 000 PLN do 850 000 PLN

2. G – wskaźnik podstawowych dochodów podatkowych na 1 mieszkańca przyjęty do obliczenia subwencji wyrównawczej w 2023 r. (https://www.gov.pl/web/finanse/wskazniki-dochodow-podatkowych-gmin-powiatow-i-wojewodztw-na-2023-r)
3. L – liczba mieszkańców w gminie za rok 2022 (Główny Urząd Statystyczny / Obszary tematyczne / Ludność / Ludność / Powierzchnia i ludność w przekroju terytorialnym w 2022 roku)
4. Eksperymentalny współczynnik najlepszego dopasowania realnej wartości grantu:

WD_{GR} = 81,9127986

5. GR – wysokość grantu, o który może ubiegać się gmina

Wzór na wysokości grantu:

$GR = L * WD_{GR}$

Jeżeli:

- GR < 200 000 PLN – należy przyjąć, że wysokość grantu wynosi 200 000 PLN, więc GR = 200 000 PLN
- GR > 850 000 PLN – należy przyjąć, że wysokość grantu wynosi 850 000 PLN, więc GR = 850 000 PLN

Metodologia wyliczenia udziału budżetu państwa

Dane wyjściowe

1. Średnia wartość wskaźnika dla kraju w 2023 r. wynosi:

$G_{śr}$ = 1 745,00 PLN

2. Minimalna wartość wskaźnika dla kraju w 2023 r. wynosi:

G_{min} = 541 PLN

3. G – wskaźnik dochodu podatkowego wybranej gminy
4. Eksperymentalny współczynnik najlepszego dopasowania realnej wartości udziału BP:

WD_{BP} = 0,04297004

5. U_{BP} – procentowy udział BP
6. W_{BP} – wkład BP

Wzór na % udział BP

$U_{BP} = 0,2 – (WD_{BP} * (G – G_{min}) / G_{śr})$

% udziału BP (U_{BP}) należy zaokrąglić w górę lub w dół do liczb całkowitych, np. 0,191234 to 19%, a 0,195111 to 20%

Wzór na określenie wkładu BP w kwocie grantu

$W_{BP} = U_{BP} * GR$

Metodologia wyliczenia wysokości wkładu własnego

Dane wyjściowe

1. Średnia wartość wskaźnika dla kraju w 2023 r. wynosi:

$G_{śr}$ = 1 745,00 PLN

2. Minimalna wartość wskaźnika dla kraju w 2023 r. wynosi:

G_{min} = 541 PLN

3. Eksperymentalny współczynnik najlepszego dopasowania realnej wartości wkładu JST:

$WD_{WWł}$ = 0,08186523

4. W_G – procentowy udział gminy, wkład własny

Wzór na % udział wkładu własnego JST

1. Jeżeli współczynnik G dla danej gminy jest równy lub większy od średniej wartości wskaźnika dla kraju ($G_{śr}$):

$G >= G_{śr}$

wówczas % udział wkładu własnego liczy się według następującego wzoru:

$W_G = WD_{WWł} * (G – G_{min}) / G_{śr}$

% udziału wkładu własnego JST może wynieść maksymalnie 20%, więc w przypadku wyższych wartości należy przyjąć 20%

2. Jeżeli współczynnik G dla danej gminy jest mniejszy od średniej wartości wskaźnika dla kraju ($G_{śr}$) wówczas % wkładu własnego gminy wynosi 0

$G < G_{śr}$

W_G = 0%

Wzór na określenie wysokości wkładu własnego JST

$W_{WWŁ} = GR * W_G / (100\% - W_G)$

Wysokość wkładu własnego JST ($W_{WWŁ}$) należy zaokrąglić w dół do liczby całkowitej, np. 12 765,90 PLN to 12 765 PLN

POWIATY

Metodologia wyliczenia udziału budżetu państwa

Dane wyjściowe

1. Średnia wartość wskaźnika dla kraju w 2023 r. wynosi:

$P_{śr}$ = 223,80 PLN

2. Minimalna wartość wskaźnika dla kraju w 2023 r. wynosi:

P_{min} = 122,14 PLN

3. P – wskaźnik dochodu podatkowego wybranego powiatu

4. Eksperymentalny współczynnik najlepszego dopasowania realnej wartości udziału BP:

WD_{BP} = 0,06973808

5. U_{BP} – procentowy udział BP

6. W_{BP} – wkład BP

7. GR – wysokość grantu, o który może ubiegać się powiat

GR = 850 000 PLN

Wzór na % udział BP

$U_{BP} = 0,2 – (WD_{BP} * (P – P_{min}) / P_{śr})$

% udziału BP (U_{BP}) należy zaokrąglić w górę lub w dół do liczb całkowitych, np. 0,191234 to 19%, a 0,195111 to 20%

Wzór na określenie wkładu BP w kwocie grantu

$W_{BP} = U_{BP} * GR$

Metodologia wyliczenia wysokości wkładu własnego

Dane wyjściowe

1. Średnia wartość wskaźnika dla kraju w 2023 r. wynosi:

$P_{śr}$ = 223,80 PLN

2. Minimalna wartość wskaźnika dla kraju w 2023 r. wynosi:

P_{min} = 122,14 PLN

3. P – wskaźnik dochodu podatkowego wybranego powiatu

4. Eksperymentalny współczynnik najlepszego dopasowania realnej wartości wkładu JST:

$WD_{WWł}$ = 0,130762

5. W_P – procentowy udział powiatu, wkład własny

Wzór na % udział wkładu własnego JST

1. Jeżeli współczynnik P dla danego powiatu jest równy lub większy od średniej wartości wskaźnika dla kraju ($P_{śr}$):

$P >= P_{śr}$

wówczas % udział wkładu własnego liczy się według następującego wzoru:

$W_P = WD_{WWł} * (P – P_{min}) / P_{śr}$

% udziału wkładu własnego JST może wynieść maksymalnie 20%, więc w przypadku wyższych wartości należy przyjąć 20%

2. Jeżeli współczynnik P dla danego powiatu jest mniejszy od średniej wartości wskaźnika dla kraju ($P_{śr}$) wówczas % wkładu własnego powiatu wynosi 0

$P < P_{śr}$

W_P = 0%

Wzór na określenie wysokości wkładu własnego JST

$W_{WWŁ} = GR * W_P / (100\% - W_P)$

Wysokość wkładu własnego JST ($W_{WWŁ}$) należy zaokrąglić w dół do liczby całkowitej, np. 12 765,90 PLN to 12 765 PLN

WOJEWÓDZTWA

Metodologia wyliczenia udziału budżetu państwa

Dane wyjściowe

1. Średnia wartość wskaźnika dla kraju w 2023 r. wynosi:

$W_{śr}$ = 339,27 PLN

2. Minimalna wartość wskaźnika dla kraju w 2023 r. wynosi:

W_{min} = 186,85 PLN

3. W – wskaźnik dochodu podatkowego wybranego województwa

4. Eksperymentalny współczynnik najlepszego dopasowania realnej wartości udziału BP:

WD_{BP} = 0,0690623

5. U_{BP} – procentowy udział BP

6. W_{BP} – wkład BP

7. GR – wysokość grantu, o który może ubiegać się województwo

GR = 850 000 PLN

Wzór na % udział BP

$U_{BP} = 0,2 – (WD_{BP} * (W – W_{min}) / W_{śr})$

% udziału BP (U_{BP}) należy zaokrąglić w górę lub w dół do liczb całkowitych, np. 0,191234 to 19%, a 0,195111 to 20%

Wzór na określenie wkładu BP w kwocie grantu

$W_{BP} = U_{BP} * GR$

Metodologia wyliczenia wysokości wkładu własnego

Dane wyjściowe

1. Średnia wartość wskaźnika dla kraju w 2023 r. wynosi:

$W_{śr}$ = 339,27 PLN

2. Minimalna wartość wskaźnika dla kraju w 2023 r. wynosi:

W_{min} = 186,85 PLN

3. W – wskaźnik dochodu podatkowego wybranego województwa

4. Eksperymentalny współczynnik najlepszego dopasowania realnej wartości wkładu JST:

$WD_{WWł}$ = 0,106205

5. W_W – procentowy udział powiatu, wkład własny

Wzór na % udział wkładu własnego JST

1. Jeżeli współczynnik P dla danego powiatu jest równy lub większy od średniej wartości wskaźnika dla kraju ($W_{śr}$):

$W >= W_{śr}$

wówczas % udział wkładu własnego liczy się według następującego wzoru:

$W_W = WD_{WWł} * (W – W_{min}) / W_{śr}$

% udziału wkładu własnego JST może wynieść maksymalnie 20%, więc w przypadku wyższych wartości należy

przyjąć 20%

2. Jeżeli współczynnik W dla danego województwa jest mniejszy od średniej wartości wskaźnika dla kraju ($W_{śr}$) wówczas % wkładu własnego województwa wynosi 0

$W < W_{śr}$

$W_W = 0\%$

<u>Wzór na określenie wysokości wkładu własnego JST</u>

$W_{WWŁ} = GR * W_W / (100\% - W_W)$

Wysokość wkładu własnego JST ($W_{WWŁ}$) należy zaokrąglić w dół do liczby całkowitej, np. 12 765,90 PLN to 12 765 PLN

6. 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 uprzywilejowanemu 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 po włamaniowej
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 jednostek 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. Kwalifikowalność kosztów tylko w okresie realizacji projektu.

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. 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.

7. 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.

8. W celu rozliczenia Grantu, Grantobiorca składa Operatorowi wniosek rozliczający za pośrednictwem aplikacji udostępnionej Grantobiorcy, do którego załącza faktury (skany, kopie), protokół/protokoły odbioru sprzętu/oprogramowania/usługi, z wyszczególnionymi ilościami oraz specyfikacją zakupionego sprzętu/oprogramowania/usług. Na potwierdzenie ubezpieczenia sprzętu zostanie przedstawiona polisa obejmująca zadeklarowany sprzęt. W zakresie potwierdzenia prawidłowości wyboru dostawców i wykonawców – na żądanie Grantodawcy, Grantobiorca przedłoży dokumentację z postępowania o udzielenie zamówienia, przeprowadzonego zgodnie z Wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2021-2027 lub ustawą z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 z późn. zm.).
9. Grantobiorca ma obowiązek dostarczenia wraz z wnioskiem rozliczającym projekt raportu z audytu oraz Ankiety stanowiącej załącznik nr 6 do Regulaminu Konkursu Grantowego.
10. Grantobiorca w ramach realizacji projektu zobowiązany jest do realizacji wskaźników zgodnie z Załącznikiem nr 9 do Regulaminu.
11. Grantobiorca jest zobowiązany do utrzymania efektów Projektu Grantowego, w tym do opracowania oraz wdrożenia procedury monitorowania utrzymania efektów Projektu Grantowego 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 datę zakończenia Projektu Grantowego rozumie się datę zaakceptowania przez Operatora końcowego rozliczenia Projektu Grantowego.
12. Grantobiorca nie posiada możliwości kwalifikowania podatku VAT w stosunku do wydatków, dla których

beneficjent odlicza ten podatek częściowo wg proporcji ustalonej zgodnie z art. 90 ust. 2 ustawy o podatku od towarów i usług (Dz.U. z 2022 r. poz. 931 z pózn. zm.). Wobec tego Grantobiorca nie ma możliwości częściowego odliczenia podatku VAT w realizowanym projekcie.

§5

Zasady i sposób wyboru Wnioskodawców

1. Nabór Wniosków o przyznanie Grantów

1) Wnioskodawcy zostaną wybrani w otwartym naborze, z zachowaniem zasady bezstronności i przejrzystości.

2) Nabór Wniosków trwać będzie od dnia **19.07.2023 r.** do dnia **13.10.2023 r. do godziny 16:00.**

   W uzasadnionych przypadkach nabór może zostać wydłużony. Beneficjent zastrzega, w razie powstania oszczędności, możliwość przeprowadzenia naboru uzupełniającego w okresie 2 tygodni. O przyznaniu dofinansowania w naborze uzupełniającym decyduje kolejność zgłoszeń do momentu wyczerpania alokacji.

3) Wszelkie zmiany o długości trwania naboru będą publikowane na Stronie internetowej Grantodawcy wraz ze wskazaniem terminów składania Wniosków o przyznanie Grantów.

2. Sposób składania Wniosków o przyznanie Grantu

1) Wzór Wniosku o przyznanie Grantu jest dostępny na Stronie internetowej Konkursu oraz stanowi załącznik nr 1 do Regulaminu.

2) Wniosek o przyznanie Grantu razem z załącznikiem nr 7 do Regulaminu Konkursu Grantowego należy wypełnić za pomocą systemu LSI, zamieszczonego na stronie internetowej konkursu pod adresem: www.gov.pl/cppc/cyberbezpieczny-samorzad.

3) Złożenie Wniosku o przyznanie Grantu jest możliwe wyłącznie przez Wnioskodawcę, który we Wniosku o przyznanie Grantu oświadczy, że zapoznał się z Regulaminem Konkursu i akceptuje jegozasady.

4) Wnioskodawca ma możliwość wycofania Wniosku o przyznanie Grantu przesyłając za pośrednictwem LSI pismo z informacją o wycofaniu z Konkursu Grantowego, podpisane elektronicznie zgodnie z reprezentacją Wnioskodawcy.

5) Wnioskodawca ma możliwość zwrócenia się z pisemną prośbą do Operatora za pośrednictwem LSI o przywrócenie terminu na złożenie Wniosku o przyznanie Grantu w przypadku wystąpienia problemów technicznych w LSI, uniemożliwiających złożenie ww. wniosku w okresie trwania naboru wniosków. Wnioskodawca zobowiązany jest wówczas do uprawdopodobnienia, że niezłożenie prawidłowo wypełnionego wniosku nastąpiło bez jego winy, a przyczyną była niemożność złożenia stosownej dokumentacji z uwagi na problemy techniczne, które wystąpiły w aplikacji służącej do kompleksowej obsługi wniosków grantowych. Wraz z wnioskiem o przywrócenie terminu, Wnioskodawca zobligowany jest przesłać Wniosek o przyznanie Grantu.

3. Sposób i zasady oceny Wniosków o przyznanie Grantu

1) Ocena będzie dokonywana przez Komisję Przyznającą Granty. Po wstępnej walidacji Wniosku o przyznanie Grantu możliwe będzie naniesienie poprawek przez Wnioskodawcę zgodnie z uwagami KPG;

2) W przypadku stwierdzenia oczywistych omyłek lub braków we Wniosku o przyznanie Grantu uniemożliwiających przeprowadzenie oceny, w tym uwzględnienia w nim wydatków niezgodnych z zakresem kosztów kwalifikowalnych zgodnie z postanowieniami §4 ust. 6, KPG skieruje za pośrednictwem LSI do Wnioskodawcy wezwanie, w zakresie omyłek/braków i sposobu ich uzupełnienia/poprawienia oraz naniesienia stosownych korekt we Wniosku o przyznanie Grantu. Wnioskodawca będzie miał 3 dni

robocze od dnia otrzymania wezwania na usunięcie oczywistej omyłki, uzupełnienie braków lub modyfikację katalogu kosztów kwalifikowalnych;

3) W przypadku braku modyfikacji katalogu kosztów kwalifikowalnych lub ich zakwestionowania przez Wnioskodawcę, KPG przekazuje Wnioskodawcy ponowne wezwanie do uzupełnienia/modyfikacji Wniosku o przyznanie Grantu w terminie 2 dni roboczych od dnia jego otrzymania wraz z adnotacją,iż niezastosowanie się do zaleceń skutkuje obniżeniem wartości kwoty dofinansowania o koszty niekwalifikowalne wskazane w wezwaniu;

4) W przypadku, gdy we Wniosku o przyznanie Grantu została określona pozycja niekwalifikująca się do sfinansowania, następuje usunięcie całej pozycji kosztowej. Jeżeli we Wniosku o powierzenie Grantu wskazano grupę kosztów niekwalifikujących się do dofinansowania w ramach danego obszaru zgodnie §3 ust. 2, kwota dofinansowania obniżana jest o 10% w ramach danego obszaru;

5) W przypadku, gdy Wnioskodawca nie zgadza się z decyzją KPG w zakresie kwalifikowalności wydatków i obniżenia wartości dofinasowania o koszty niekwalifikowalne, ma możliwość wycofaniawniosku z Konkursu Grantowego, zgodnie z §5 ust. 2 pkt. 4). Jednocześnie brak wycofania wniosku z Konkursu jest jednoznaczny z zaakceptowaniem decyzji KPG w zakresie wysokości otrzymania dofinansowania;

6) Jeżeli Wnioskodawca nie poprawi lub nie uzupełni Wniosku o przyznanie Grantu w terminie lub zakresie wskazanym w wezwaniu, o którym mowa w pkt 2, ocena Projektu Grantowego prowadzona jest na podstawie złożonego Wniosku o przyznanie Grantu;

7) W przypadku stwierdzenia omyłek lub braków we Wniosku o przyznanie Grantu, które nie uniemożliwiają dokonania oceny Wniosku o przyznanie Grantu, dopuszcza się skorygowanie stwierdzonych błędów przy zawarciu Umowy o powierzenie Grantu;

8) Wnioski o przyznanie Grantu zostaną poddane ocenie formalno-merytorycznej w oparciu o kryteriawyboru projektów grantowych, określone w załączniku nr 3 do Regulaminu;

9) Oceny formalno-merytorycznej Wniosku o przyznanie Grantu dokonuje KPG;

10) W skład KPG wchodzą pracownicy Operatora w tym: Przewodniczący, Sekretarz i co najmniej dwóch Oceniających;

11) Ocena Wniosków o przyznanie Grantu trwa ok. 60 dni, liczonych od dnia złożenia wniosku w trakcie prowadzonego naboru wniosków o przyznanie Grantów;

12) Prawdziwość oświadczeń i danych zawartych we Wniosku o przyznanie Grantu może zostać zweryfikowana w trakcie weryfikacji warunków formalnych i oceny, jak również przed i po zawarciuUmowy o powierzenie Grantu;

13) Wnioskodawca ma prawo dostępu do dokumentów grantowych związanych z oceną złożonego przez siebie Wniosku o przyznanie Grantu, z zastrzeżeniem, że dane osobowe członków KPG dokonujących oceny nie podlegają ujawnieniu;

14) Wyniki oceny formalno-merytorycznej zostaną opublikowane na Stronie internetowej Projektu, zaś informacja o zakończeniu oceny zostanie wysłana przez LSI do Wnioskodawców;

15) Projekt może zostać wybrany do dofinansowania, jeżeli jednocześnie:

    a) spełnił kryteria wyboru projektów i uzyskał wymaganą liczbę punktów,

    b) Wnioskodawca nie został wykluczony z możliwości otrzymania dofinansowania zgodnie z art. 37 ust. 3 ustawy wdrożeniowej;

16) Członkowie KPG są zobowiązani do złożenia oświadczenia o bezstronności i braku osobistegointeresu w procesie oceny. Za konflikt interesów uważa się jakiekolwiek przesłanki osobiste, rodzinne, zawodowe,

finansowe czy innej natury mogące przeszkodzić w bezstronnej ocenie Wniosku o przyznanie Grantu.

§6

Zawarcie Umowy o powierzenie Grantu

1. Wzór Umowy o powierzenie Grantu stanowi załącznik nr 4 do Regulaminu.
2. Wraz z informacją o wyborze Projektu Grantowego do dofinansowania, Operator wzywa Wnioskodawcę za pośrednictwem LSI, do dostarczenia dokumentów niezbędnych do zawarcia Umowy o powierzenie Grantu, wymienionych w załączniku nr 5 do Regulaminu.
3. Umowa o powierzenie Grantu zostaje zawarta w formie elektronicznej.
4. Wnioskodawca dostarcza dokumenty niezbędne do zawarcia Umowy o powierzenie Grantu w terminie 14 dni od dnia otrzymania przez Wnioskodawcę wezwania, o którym mowa w ust. 2. W przypadku niedostarczenia kompletnych co do formy i treści dokumentów w tym terminie, Operator może odmówić zawarcia Umowy o powierzenie Grantu.

§7

Postanowienia końcowe

1. Składając Wniosek o przyznanie Grantu, Wnioskodawca akceptuje zasady Konkursu Grantowego zawarte w niniejszym Regulaminie.
2. Odpowiedzi na najczęstsze pytania dotyczące Konkursu Grantowego będą publikowane w pytaniach i odpowiedziach na stronie: www.gov.pl/cppc/cyberbezpieczny-samorzad.
3. Ewentualne pytania dotyczące Konkursu Grantowego Wnioskodawcy mogą zgłaszać na **adres e-mail: 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.
4. W sprawach nieuregulowanych niniejszym Regulaminem mają zastosowanie powszechnie obowiązujące przepisy prawa.
5. W przypadku zmiany Regulaminu, Centrum Projektów Polska Cyfrowa zamieszcza na Stronie internetowej Projektu informację o jego zmianie.
6. Centrum Projektów Polska Cyfrowa zastrzega możliwość anulowania Konkursu Grantowego, w szczególności w przypadku wprowadzenia istotnych zmian w przepisach prawa mających wpływ na warunki przeprowadzenia konkursu lub zaistnienia zdarzeń o charakterze siły wyższej.

Załączniki:

1. Wzór Wniosku o przyznanie Grantu (Formularz Aplikacyjny);
2. Lista podmiotów uprawnionych do uczestniczenia w naborze;
3. Kryteria wyboru projektów grantowych;
4. Wzór Umowy o powierzenie Grantu;
5. Lista dokumentów niezbędnych do podpisania Umowy o powierzenie Grantu;
6. Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych);
7. Oświadczenie dotyczące kwalifikowalności podatku VAT;
8. Klauzula informacyjna FERC;
9. Opis wskaźników projektu Cyberbezpieczny Samorząd.