Regulamin Konkursu Grantowego pn. „Cyberbezpieczny Samorząd”

Priorytet II: Zaawansowane usługi cyfrowe.

Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

Warszawa, 16.06.2026 r.

§1 Słownik pojęć:

Ankieta - „Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", dokument opracowany przez Operatora, na potrzeby oceny poziomu dojrzałości cyberbezpieczeństwa u Grantobiorcy, dostępna na stronie internetowej Konkursu pn. „Cyberbezpieczny Samorząd", wypełniana przez Grantobiorcę po zawarciu Umowy o powierzenie grantu oraz przy składaniu Wniosku rozliczającego i każdorazowo przekazywana Operatorowi, stanowiąca załącznik nr 6 do dokumentacji konkursowej.

FERC – program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, przyjęty decyzją wykonawczą Komisji Europejskiej z dnia 18 listopada 2022 r.

Grant – należy przez to rozumieć środki finansowe przekazane Grantobiorcy na podstawie Umowy o powierzenie grantu, przeznaczone na realizację zadań określonych w Projekcie, służących osiągnięciu celów Projektu grantowego, zgodnie z art. 41 ust. 5 ustawy wdrożeniowej.

Grantobiorca – podmiot będący jednostką samorządu terytorialnego, o którym mowa w art. 41 ust. 3 ustawy wdrożeniowej, wybrany w procesie otwartego naboru, ogłoszonego przez Beneficjenta;

Grantodawca lub Beneficjent – podmiot, o którym mowa w art. 41 ust. 8 ustawy wdrożeniowej, Centrum Projektów Polska Cyfrowa;

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

Komisja Przyznająca Granty lub KPG – komisja zatwierdzająca listę rankingową Wniosków o przyznanie grantu według zasad określonych w niniejszym Regulaminie;

Konkurs Grantowy lub Konkurs – otwarty nabór, o którym mowa w art. 41 ust. 3 ustawy wdrożeniowej prowadzony przez Operatora w celu wyłonienia Grantobiorców;

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

Operator lub **Partner** – podmiot, o którym mowa w art. 39 ust. 2 ustawy wdrożeniowej, czyli Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;

Projekt – przedsięwzięcie opisane we Wniosku o przyznanie grantu, realizowane przez Grantobiorcę na podstawie Umowy o powierzenie grantu i finansowane z Grantu na zasadach określonych w Umowie o powierzenie grantu, służące realizacji celów Projektu grantowego.

Projekt grantowy – projekt, o którym mowa w art. 41 ust. 2 ustawy wdrożeniowej, realizowany przez Beneficjenta pod nazwą „Cyberbezpieczny Samorząd" o numerze FERC.02.02-IP.01-0001/23 w ramach którego Beneficjent za pośrednictwem Operatora, udziela Grantobiorcom Grantów na realizację zadań służących osiągnięciu celu tego Projektu;

Regulamin Konkursu Grantowego lub Regulamin – niniejszy Regulamin naboru;

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

SZOP - Szczegółowy Opis Priorytetów Programu FERC;

Umowa o powierzenie grantu – umowa, o której mowa w art. 41 ust. 7 ustawy wdrożeniowej zawarta pomiędzy Grantobiorcą i Grantodawcą określająca w szczególności przedmiot umowy, zadania Grantobiorcy objęte Grantem, kwotę Grantu, okres realizacji Projektu, 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. z 2025 r. poz. 1733 z późn. zm.);

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

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

Wskaźniki projektu – wartości docelowe oraz miary realizacji Projektu, określone w Załączniku nr 9 do Regulaminu Konkursu Grantowego, których osiągnięcie jest obowiązkiem Grantobiorcy.

§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 z 2021 Nr 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 2025 r. poz. 1733 z późn. zm.);
    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 (tj. Dz. U. z 2024 r. poz. 1725);
    5) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2026 r. poz. 252).

§3 Informacje ogólne

1. Celem Konkursu Grantowego jest wybór podmiotów, którym zostanie udzielony Grant na realizację zadań służących osiągnięciu celu Projektu grantowego.
   Celem Projektu grantowego jest wsparcie JST w zakresie realizacji usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji JST wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem

placówek ochrony zdrowia) w kontekście zwiększenia poziomu cyberbezpieczeństwa. Cel Projektu grantowego wpisuje się w cele FERC oraz cele określone w SZOP.

2. Grantodawca przyzna Grantobiorcy Grant na zadania w ramach poniżej wskazanych obszarów:

    1) **obszar organizacyjny** - środki można przeznaczyć na następujące działania (usługi):
        a) 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.,
        b) 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):
        a) podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST,
        b) szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji (SZBI),
        c) szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu,
        d) 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):
   a) zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta,
   b) 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,
   c) zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa,
   d) zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa,
   e) zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych,
   f) 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 (SZBI) obejmującego system bezpieczeństwa informacji (SBI).

4. Obowiązek ten ciąży na kierownictwie podmiotu publicznego na podstawie § 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”, i realizowany jest zgodnie z poniższymi warunkami:

1) zakres audytu systemu bezpieczeństwa informacji (SBI) 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 (SBI) wdrożonego w urzędzie JST i dostarczony do Grantobiorcy;
3) niezwłocznie po sporządzeniu raportu z audytu, Grantobiorca zobowiązany jest uzupełnić Wniosek rozliczający Grant 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 (SBI) 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 (SBI) oraz przekazanie raportu do Operatora wraz z załącznikiem nr 6 do Regulaminu Konkursu Grantowego, następuje na zakończenie realizacji Projektu (jako załączniki do Wniosku rozliczającego Grant).

5. Niniejszy Regulamin określa szczegółowe zasady powierzania Grantów w ramach Konkursu Grantowego.

6. Konkurs Grantowy jest prowadzony na terenie całej Polski.

7. Konkurs Grantowy przeprowadzany jest jawnie, z zapewnieniem publicznego dostępu do informacji o zasadach jego przeprowadzania oraz listy rankingowej Projektów, które otrzymały Grant.

8. Nabór Wniosków odbędzie się w ramach otwartego naboru grantowego.

9. Grantobiorcy będą realizowali Projekty na podstawie Umowy o powierzenie grantu, zawartej z Grantodawcą.

10. Warunki dotyczące okresu realizacji Projektu:

    1) okres realizacji Projektu określany jest w Umowie o powierzenie grantu i nie może trwać dłużej niż do dnia **30.09.2026 r.**

    2) Grantobiorca i Grantodawca mogą w Umowie o powierzenie grantu uzgodnić krótszy okres realizacji Projektu, o ile wynika to z postanowień Umowy o powierzenie grantu.

11. Warunki dotyczące okresu kwalifikowalności:

    1) kwalifikowalność wydatków obejmuje wydatki poniesione w okresie od dnia **1.06.2023 r**. do dnia **30.09.2026 r**.

    2) w przypadku uzgodnienia przez Grantobiorcę i Grantodawcę krótszego okresu realizacji Projektu, o którym mowa w § 3 ust. 10 pkt 2 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.

    3) jeżeli wydatek (w szczególności wydatek na wartości niematerialne i prawne) obejmuje okres wykraczający poza okres kwalifikowalności wydatków określony odpowiednio zgodnie z § 3 ust. 11 pkt 1 lub 2, będzie on kwalifikowalny

wyłącznie w części proporcjonalnej do okresu kwalifikowalności wydatków.

12. 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.

Na podstawie przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2026 r. poz. 20) krajowy system cyberbezpieczeństwa obejmuje podmioty publicznej, w tym 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 2025 poz. 1483 z późn. zm.).

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

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.

§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 grantu publikowaną w dniu ogłoszenia naboru.

2. 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).**

3. Maksymalna intensywność dofinansowania Projektu „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/województwa przyjęty 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. (Wskaźniki dochodów podatkowych);
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} = 541,00 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. WG – procentowy udział gminy, wkład własny.

Wzór na % udział wkładu własnego JST:

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: $WG = WD_{WWł} * (G – G_{min}) / G_{śr}$.
  % udziału wkładu własnego JST może wynieść maksymalnie 20%, więc w przypadku wyższych wartości należy przyjąć 20%;
- współczynnik G dla danej gminy jest mniejszy od średniej wartości wskaźnika dla kraju ($G_{śr}$) wówczas % wkładu własnego gminy wynosi 0: G < $G_{śr}$ to 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. WP – procentowy udział powiatu, wkład własny.

Wzór na % udział wkładu własnego JST:

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%
- współczynnik P dla danego powiatu jest mniejszy od średniej wartości wskaźnika dla kraju ($P_{śr}$) wówczas % wkładu własnego powiatu wynosi 0: P < $P_{śr}$, to $W_P = 0\%$

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:

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%;
- współczynnik W dla danego województwa jest mniejszy od średniej wartości wskaźnika dla kraju ($W_{śr}$) wówczas % wkładu własnego województwa wynosi 0: W < $W_{śr}$, to W_W = 0%.

Wzór na określenie wysokości wkładu własnego JST: $W_{WWŁ} = GR * W_W / (100\% - W_W)$.

Wysokość wkładu własnego JST (WWWŁ) 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:
      - 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, o którym mowa w § 3 ust. 11 pkt 1 albo 2, i proporcjonalnie do okresu kwalifikowalności wydatków w Projekcie:

- 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.

7. Do wydatków niekwalifikowalnych w ramach Grantu 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.

8. W celu rozliczenia Grantu, Grantobiorca składa Operatorowi Wniosek rozliczający Grant 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 Ministra Funduszy i Polityki Regionalnej dotyczącymi kwalifikowalności wydatków na lata 2021-2027 lub ustawą z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.).

9. Grantobiorca ma obowiązek dostarczenia, wraz z Wnioskiem rozliczającym Grant, raportu z audytu oraz Ankiety Dojrzałości Cyberbezpieczeństwa 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, 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.

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

13. Grantobiorca nie posiada możliwości kwalifikowania podatku VAT w stosunku do wydatków, dla których odlicza się ten podatek częściowo wg proporcji ustalonej zgodnie z art. 90 ust. 2 ustawy o podatku od towarów i usług (Dz.U. z 2025 r. poz.

77 z późn. zm.). Wobec tego Grantobiorca nie ma możliwości częściowego odliczenia podatku VAT w realizowanym Projekcie.

§5 Zasady i sposób wyboru Wnioskodawców grantu

1. **Nabór Wniosków o przyznanie Grantów:**

   1) Wnioskodawcy grantu zostaną wybrani w otwartym naborze, z zachowaniem zasady bezstronności i przejrzystości.
   2) Nabór Wniosków trwać będzie od **19.07.2023 r.** do **14.12.2023 r**. do godziny **16:00**.
      W uzasadnionych przypadkach nabór może zostać wydłużony. Beneficjent zastrzega w razie powstania oszczędności, możliwość przeprowadzenia naboru uzupełniającego. O przyznaniu Grantu 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 Grantowego 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 Grantowego pod adresem: www.gov.pl/cppc/cyberbezpieczny-samorzad.
   3) Złożenie Wniosku o przyznanie grantu jest możliwe wyłącznie przez Wnioskodawcę grantu, który we Wniosku o przyznanie grantu oświadczy, że zapoznał się z Regulaminem Konkursu i akceptuje jego zasady.
   4) Wnioskodawca grantu 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 grantu.

5) Wnioskodawca grantu 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 grantu 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 o przyznanie grantu. Wraz z wnioskiem o przywrócenie terminu, Wnioskodawca grantu zobligowany jest przesłać Wniosek o przyznanie grantu.
6) Wnioskodawca grantu ma możliwość zwrócenia się z prośbą do Operatora o zmianę kontekstu dla konta w systemie LSI nie później niż 7 dni przed planowanym zakończeniem naboru do Konkursu Grantowego.
7) Wnioskodawca grantu uprawniony jest do złożenia jednego wniosku w Konkursie Grantowym. W przypadku złożenia większej ilości wniosków, oceniany będzie ten złożony jako pierwszy.

1. 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 grantu 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 grantu wezwanie, w zakresie omyłek/braków i sposobu ich uzupełnienia/poprawienia oraz naniesienia

stosownych korekt we Wniosku o przyznanie grantu. Wnioskodawca grantu będzie miał 5 dni kalendarzowych 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 grantu, KPG przekazuje Wnioskodawcy grantu ponowne wezwanie do uzupełnienia/modyfikacji Wniosku o przyznanie grantu w terminie 4 dni kalendarzowych od dnia jego otrzymania wraz z adnotacją, iż niezastosowanie się do zaleceń skutkuje obniżeniem wartości kwoty Grantu 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 z §3 ust. 2, kwota dofinansowania obniżana jest o 10% w ramach danego obszaru;
5) W przypadku, gdy Wnioskodawca grantu nie zgadza się z decyzją KPG w zakresie kwalifikowalności wydatków i obniżenia wartości dofinansowania o koszty niekwalifikowalne, ma możliwość wycofania Wniosku z Konkursu Grantowego, zgodnie z §5 ust. 2 pkt. 4). Jednocześnie brak wycofania Wniosku z Konkursu Grantowego jest jednoznaczne z zaakceptowaniem decyzji KPG w zakresie wysokości otrzymania dofinansowania;
6) Jeżeli Wnioskodawca grantu nie poprawi lub nie uzupełni Wniosku o przyznanie grantu w terminie lub zakresie wskazanym w wezwaniu, o którym mowa w pkt 2, KPG ocenia złożony Wniosek 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 kryteria wyboru Projektów, 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;
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 zawarciu Umowy o powierzenie grantu;
13) Wnioskodawca grantu ma prawo dostępu do dokumentów 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 Grantowego, zaś informacja o zakończeniu oceny zostanie wysłana przez LSI do Wnioskodawców grantu;
15) Projekt może oceniony pozytywnie, jeżeli jednocześnie:
    a) spełnił kryteria wyboru Projektów i uzyskał wymaganą liczbę punktów,
    b) Wnioskodawca grantu nie został wykluczony z możliwości otrzymania Grantu w rozumieniu art. 41 ust. 4 ustawy wdrożeniowej;
16) Członkowie KPG są zobowiązani do złożenia oświadczenia o bezstronności i braku osobistego interesu 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 przyznaniu Grantu, Operator wzywa Wnioskodawcę grantu 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.

Wnioskodawca grantu dostarcza dokumenty niezbędne do zawarcia Umowy o powierzenie grantu w terminie 14 dni od dnia otrzymania przez Wnioskodawcę grantu wezwania, o którym mowa w ust. 2. W przypadku niedostarczenia kompletnych co do formy i treści dokumentów w tym terminie, Operator może odmówić przyjęcia dokumentów jako spełniających warunki do zawarcia Umowy o powierzenie Grantu, co skutkuje brakiem możliwości zawarcia Umowy przez Grantodawcę.

§7 Postanowienia końcowe

1. Składając Wniosek o przyznanie grantu, Wnioskodawca grantu 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 grantu 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, Grantodawca zamieszcza na stronie internetowej Projektu grantowego informację o jego zmianie.
6. Grantodawca zastrzega sobie 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;
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.