SCHEMAT GRANTOWY
dla Projekt pod nazwą „Cyberbezpieczny Rząd”

CEL DOKUMENTU

Niniejszy dokument określa minimalny zakres procedur udzielania grantów przez Ostatecznego Odbiorcę Wsparcia i Partnera w Projekcie.

Realizacja Konkursu Grantowego pn. „**Cyberbezpieczny Rząd**” odbywa się w formie szeregu projektów grantowych zgodnie z Projektem przewidzianym w opisie Inwestycji **C3.1.1.** Cyberbezpieczeństwo – CyberPL infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo.

Projekt – “Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach teleinformatycznych (TI), w tym wsparcie podmiotów wykorzystujących technologie teleinformacyjne (TI) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)”.

Projekt grantowy – pojedynczy Projekt podejmowany, realizowany i rozliczony przez Grantobiorcę w ramach Konkursu Grantowego.

WYBÓR PROJEKTÓW GRANTOWYCH DO UDZIELENIA GRANTU

RAMOWE KRYTERIA WYBORU GRANTOBIORCÓW

Wnioski o przyznanie grantu na realizację projektów grantowych zostaną poddane ocenie formalnej i merytorycznej w oparciu o określone kryteria wyboru. W zakresie oceny formalnej zostanie zweryfikowane, czy Wnioskodawca i Wniosek spełniają zdefiniowane kryteria oceny formalnej. Za spełnienie każdego z kryteriów zostanie przyznany jeden punkt (zasada nie spełnia/spełnia). Wnioskodawca musi spełniać wszystkie kryteria formalne, aby jego Wniosek o przyznanie grantu został oceniony pozytywnie w ocenie formalnej i mógł zostać poddany ocenie merytorycznej. W zakresie oceny merytorycznej zostanie zweryfikowane czy Wniosek w części merytorycznej spełnia zdefiniowane kryteria oceny merytorycznej. Za spełnienie każdego z kryteriów 1, 2, 3 zostanie przyznany jeden punkt (zasada nie spełnia/spełnia). Wniosek musi spełniać każde z tych kryteriów i uzyskać maksymalną liczbę punktów. W zakresie kryterium 4 Ocena planowanego zakresu postępu Projektu grantowego zostanie przyznana pula punktów odpowiadająca wykazanemu postępowi budowania odporności na cyberzagrożenia na bazie wskazanych rozwiązań bezpieczeństwa, które będą przedmiotem wdrożenia lub rozbudowy w ramach Projektu grantowego. W przypadku otrzymania przez kilku Wnioskodawców takiej samej liczby punktów w ramach przeprowadzonej oceny merytorycznej, o wyborze projektu grantowego decyduje kolejność złożenia Wniosku przez Wnioskodawcę.

Kryteria oceny formalnej:

Lp.	Nazwa kryterium formalnego	Opis kryterium	Sposób oceny
1	Kwalifikowalność Wnioskodawcy	Weryfikacji podlega czy Wnioskodawca grantowy jest podmiotem krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie	0-1 (nie spełnia/spełnia)

Lp.	Nazwa kryterium formalnego	Opis kryterium	Sposób oceny
		cyberbezpieczeństwa, tj.: – Wojewodami, – Centralnymi lub naczelnymi organami administracji rządowej zgodnie z załącznikiem nr 1 do Regulaminu Konkursu (Lista podmiotów wskazanych w Załączniku nr 1 nie stanowi katalogu zamkniętego) oraz czy Wniosek został złożony w trakcie prowadzonego naboru.	
2	Niepodleganie wykluczeniu z możliwości otrzymania finansowania ze środków Unii Europejskiej	Weryfikacji podlega czy Wnioskodawca grantowy nie został wykluczony z możliwości otrzymania finansowania ze środków UE - kryterium weryfikowane na podstawie oświadczeń zawartych we Wniosku o przyznanie grantu.	0-1 (nie spełnia/spełnia)
3	Wysokość wnioskowanej kwoty	Weryfikacji podlega czy wnioskowana kwota nie przekracza maksymalnej kwoty wskazanej w Regulaminie Konkursu Grantowego. Wysokość grantu dla jednego	0-1 (nie spełnia/spełnia)

Lp.	Nazwa kryterium formalnego	Opis kryterium	Sposób oceny
		Wnioskodawcy uzależniona jest od wskazanej przez niego i objętej Projektem grantowym liczby jednostek mu podległych.	
4	Okres realizacji Projektu grantowego	Okres realizacji Projektu grantowego nie przekracza terminu wskazanego w Regulaminie Konkursu Grantowego.	0-1 (nie spełnia/spełnia)
5	Zapewnienie zachowania efektów długoterminowych Projektu grantowego	Weryfikacji podlega czy zachowane zostaną efekty długoterminowe, tj. utrzymane przez okres 3 lat od zakończenia Projektu grantowego. Ocena na podstawie oświadczenia Wnioskodawcy grantowego o zapoznaniu się z Regulaminem Konkursu Grantowego i akceptacji jego zasad, zawartych we Wniosku o przyznanie grantu.	0-1 (nie spełnia/spełnia)
6	Zgodność z celem Projektu	Weryfikacji podlega, czy przedstawiony przez Wnioskodawcę grantowego opis koncepcji Projektu grantowego zawiera zapisy potwierdzające zgodność z celami i efektami Projektu, w tym w odniesieniu do celów zgodnych z opisem Inwestycji C3.1.1.	0-1 (nie spełnia/spełnia)

Lp.	Nazwa kryterium formalnego	Opis kryterium	Sposób oceny
		Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo.	
7	Zgodność Projektu grantowego z zasadami horyzontalnymi	Weryfikacji podlega, czy Wnioskodawca ubiegający się o grant wskazał, iż w toku realizacji Projektu grantowego zapewni zgodność z: – zasadą równości szans i niedyskryminacji oraz zasadą równości szans kobiet i mężczyzn, – zasadą „niewyrządzania znaczącej szkody środowisku” (DNSH – „do no significant harm”), – zasadą zrównoważonego rozwoju - racjonalne wykorzystywanie zasobów naturalnych. a przedstawione we Wniosku uzasadnienia są wyczerpujące.	0-1 (nie spełnia/spełnia)

Kryteria oceny merytorycznej:

l.p.	Nazwa kryterium merytorycznego	Opis kryterium	Sposób oceny
1	Kwalifikowalność wydatków	Weryfikacji podlega czy wskazane we Wniosku wydatki są kwalifikowalne i zgodne z Regulaminem Konkursu Grantowego.	0-1 (nie spełnia/spełnia)
2	Zasadność kosztów w Projektu grantowym	Weryfikacji podlega czy Wnioskodawca grantowy wystarczająco uzasadnił potrzebę wskazanych wydatków oraz ich racjonalność w kontekście celu Projektu grantowego oraz potrzeb Wnioskodawcy.	0-1 (nie spełnia/spełnia)
3	Opis koncepcji Projektu grantowego	Weryfikacji podlega czy Wnioskodawca grantowy w sposób kompletny wypełnił Wniosek, odnosząc się do wszystkich zadań i rozwiązań bezpieczeństwa, wskazując produkty i usługi, charakterystykę i opis rozwiązania, ocenę zakresu i poziomu rozwiązań bezpieczeństwa, tak dla stanu obecnego, jak też dla stanu planowanego do osiągnięcia w wyniku realizacji Projektu grantowego.	0-1 (nie spełnia/spełnia)

4	Ocena planowanego zakresu postępu Projektu grantowego	Weryfikacji podlega zadeklarowany przez Wnioskodawcę zakres postępu budowania odporności na cyberzagrożenia na bazie wskazanych rozwiązań bezpieczeństwa, które będą przedmiotem wdrożenia lub rozbudowy w ramach Projektu grantowego.	0-61,5

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

Informacja o naborze wniosków

Informacja o naborze wniosków, zasady konkursu i link do aplikacji służącej do składania wniosków zostaną opublikowane na stronie CPPC – **Cyberbezpieczny Rząd**.

Nabór wniosków w ramach otwartego Konkursu Grantowego

Nabór wniosków odbędzie się w ramach otwartego naboru grantowego, ogłaszanego na stronie **Cyberbezpieczny Rząd**. Nabór skierowany będzie do podmiotów krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tj.:

- **Wojewodowie,**
- **Centralne lub naczelne organy administracji rządowej**.

Nabór wniosków potrwa od 28.02.2025 r. do 31.03.2025 r. (do godziny 16:00).

Przewidywana liczba grantów i alokacja

1. Alokacja na granty w Konkursie Grantowym pn. “Cyberbezpieczny Rząd” wynosi **350 000 000 PLN netto** (w tym środki unijne w wysokości **350 000 000 PLN netto**).

2. Maksymalna wysokość przyznanego grantu dla Projektu grantowego może wynosić **do 100% kosztów kwalifikowalnych**.

3. Minimalna wysokość grantu dla jednego Grantobiorcy wynosi **500 000 PLN netto**, natomiast maksymalna wysokość Grantu wynosi **10 000 000,00 PLN netto**. Wysokość grantu dla jednego Wnioskodawcy grantowego uzależniona jest od wskazanej liczby jednostek mu podległych.

4. Wnioskodawca grantowy, który wskazał wsparcie **do 4 (czterech) jednostek podległych włącznie**, może ubiegać się o wsparcie w wysokości **do 5 000 000,00 PLN netto.** Wnioskodawca grantowy, który wskazał wsparcie **5 (pięć lub więcej) jednostek podległych**, może ubiegać się o wsparcie w wysokości **do 10 000 000,00 PLN netto.**

5. VAT nie jest wydatkiem kwalifikowalnym i nie może być finansowany w ramach Projektu jak i projektów grantowych realizowanych przez Grantobiorców.

6. Wysokość przyznanego grantu dla poszczególnych jednostek może zostać zwiększona powyżej wartości określonej w Regulaminie Konkursu Grantowego i ogłoszona przez OOW w przypadku ewentualnego naboru uzupełniającego określonego zgodnie z zapisami wskazanymi w Regulaminie Konkursu Grantowego.

7. Przewidywana liczba jednostek objętych wsparciem to minimum 48 **podmiotów** krajowego systemu cyberbezpieczeństwa (KSC) wraz z jednostkami podległymi łącznie, z zastrzeżeniem, że wsparcie może zostać udzielone do wyczerpania alokacji wskazanej w Konkursie Grantowym. Maksymalna liczba jednostek mogących ubiegać się o wsparcie wraz z jednostkami podległymi wynosi **500 podmiotów**.

Sposób składania wniosków

Wnioski składane są w formie elektronicznej za pośrednictwem LSI - aplikacji do składania wniosków dostępnej na stronie Cyberbezpieczny Rząd oraz LSI – Lokalny System Informatyczny.

Sposób i zasady oceny wniosków

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

WYDATKI KWALIFIKOWALNE I SPOSÓB ROZLICZANIA GRANTÓW

Katalog kosztów kwalifikowalnych

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	Symbol produktu
1	Firewall sieciowy	S01
2	NGFW (Next Gen. Firewall)	S02
3	WAF (Web Application Firewall)	S03

4	SIEM (Security Information and Event Management)	S04
5	SOAR (Security Orchestration, Automation and Response)	S05
6	HoneyPot	S06
7	UTM (Unified Threat Management)	S07
8	IPS (Intrusion Prevention System)	S08
9	IDS (Intrusion Detection System)	S09
10	VPN (Virtual Private Network)	S10
11	NAC (Network Access Control)	S11
12	Proxy sprzętowe	S12
13	Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA	S13
14	Serwer do wykonywania kopii zapasowych (w tym z usługą/licencją deduplikacji)	S14
15	Napęd Streamer i/lub kasety do Stramera	S15

16	Macierz dyskowa	S16
17	Dyski twarde do macierzy dyskowej	S17
18	Dyski twarde do serwerów, w których będą zainstalowane kwalifikowalne systemy z zakresu bezpieczeństwa	S18
19	Pamięć RAM do serwerów, w których będą zainstalowane kwalifikowalne systemy z zakresu bezpieczeństwa	S19
20	Procesor do serwerów, w których będą zainstalowane kwalifikowalne systemy z zakresu bezpieczeństwa	S20
21	Network Attached Storage (NAS)	S21
22	Storage Area Network (SAN)	S22
23	Web Secure Gateway	S23
24	Email Secure Gateway	S24
25	Urządzenia sprzętowe Sandbox	S25
26	Ochrona AntyDDoS	S26
27	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu	S27

	802.1X (switch)	
28	Zarządzalne centralnie urządzenie sieciowe WiFi	S28
29	Access Pointy WiFi	S29
30	System monitorujący pracę urządzeń sieciowych i serwerów	S30
31	Klucze sprzętowe U2F	S31
32	Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa	S32
33	Urządzenia do zabezpieczania dowodów cyfrowych	S33
34	Urządzenia HSM	S34

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 grantowego:

L.p.	**Nazwa produktu**	**Symbol produktu**
1	Oprogramowanie antywirusowe	O01

2	Oprogramowanie Firewall	O02
3	Oprogramowanie NGFW (Next Gen Firewall)	O03
4	Oprogramowanie UTM (Unified Threat Management)	O04
5	Oprogramowanie IPS (Intrusion Prevention System)	O05
6	Oprogramowanie IDS (Intrusion Detection System)	O06
7	Oprogramowanie VPN (Virtual Private Network)	O07
8	Oprogramowanie NAC (Network Access Control)	O08
9	Oprogramowanie typu MDM (Mobile Device Management)	O09
10	Oprogramowanie typu EDR (Endpoint Detection and Response)	O10
11	Oprogramowanie typu XDR (Extended Detection and Response)	O11
12	Oprogramowanie typu NDR (Network Detection & Response)	O12
13	Oprogramowanie typu ITDR (Identity Threat Detection and Response)	O13
14	Oprogramowanie do wykonywania kopii zapasowych (w tym deduplikacji)	O14
15	Oprogramowanie antyspamowe	O15
16	Oprogramowanie WAF (Web Application Firewall)	O16

17	Oprogramowanie SIEM (Security Information and Event Management)	O17
18	Oprogramowanie SOAR (Security Orchestration, Automation and Response)	O18
19	Oprogramowanie SASE VPN	O19
20	Oprogramowanie typu Network Security Policy Management & Orchestration	O20
21	Oprogramowanie HoneyPot	O21
22	Oprogramowanie Menadżera logów	O22
23	Oprogramowanie do zarządzania podatnościami	O23
24	Oprogramowanie przeciwdziałające wyciekowi danych (DLP – Data Leak Prevention)	O24
25	Oprogramowanie do zarządzania uprzywilejowanym dostępem (PAM- Privileged Access Management/ PIM - Privileged Identity Management)	O25
26	Oprogramowanie typu BAS (Breach and attack simulation)	O26
27	Oprogramowanie Web Secure Gateway	O27
28	Oprogramowanie Email Secure Gateway	O28
29	Oprogramowanie do zarządzania tożsamością i dostępem	O29
30	Oprogramowanie centralnego menadżera haseł	O30
31	Oprogramowanie do monitorowania infrastruktury informatycznej	O31
32	Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych	O32
33	Oprogramowanie do badania podatności systemów informatycznych	O33
34	Oprogramowanie do badania podatności serwisów WWW	O34
35	Oprogramowanie do badania podatności w kodzie aplikacji	O35
36	Oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików	O36
37	Oprogramowanie do analizy powłamaniowej	O37
38	Oprogramowanie do ochrony przed ransomware	O38
39	Oprogramowanie typu ITSM (Information Technology Service Management)	O39
40	Oprogramowanie typu SoftHSM	O40
41	Oprogramowanie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie)	O41
42	Certyfikaty SSL serwisów internetowych	O42
43	Oprogramowanie ochrony AntyDDoS	O43
44	System wirtualizacyjny, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu bezpieczeństwa	O44
45	System operacyjny i/lub licencje dostępowe (również rozbudowa licencji	O45

	do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu bezpieczeństwa	

3) **usługi zewnętrzne, w szczególności**:

a) merytoryczne przygotowanie Projektu grantowego przez osoby lub podmioty zewnętrzne, w których osoba/-y odpowiedzialna za przygotowania Projektu posiadają stosowną wiedzę i m.in. 2-letnie doświadczenie we wnioskowanym zakresie oraz co najmniej 1 (jeden) certyfikat świadczący o posiadanej wiedzy w danym zakresie. Kwalifikowalność kosztów tylko w okresie realizacji Projektu grantowego;

b) usługi informatyczne i szkolenia zwiększające poziom bezpieczeństwa informacji, tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach teleinformatycznych. Kwalifikowalność kosztów tylko w okresie realizacji Projektu grantowego. Wykaz usług:

L.p.	**Nazwa usługi**	**Symbol produktu**
1	Usługa poczty elektronicznej w chmurze obliczeniowej typu IaaS, SaaS, PaaS z rozwiązaniami bezpieczeństwa	U01
2	Testy bezpieczeństwa infrastruktury sieciowej	U02
3	Testy bezpieczeństwa serwisów internetowych	U03
4	Testy bezpieczeństwa aplikacji	U04
5	Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS w zakresie	U05

	sandbox do badania bezpieczeństwa aplikacji oraz plików	
6	Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego	U06
7	Usługa w chmurze obliczeniowej SASE VPN	U07
8	Usługa w chmurze obliczeniowej MDM (Mobile Device Management)	U08
9	Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source.	U09
10	Utrzymanie i eksploatacja urządzeń/oprogramowania/rozwiązania zzakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source.	U10
11	Usługa typu MDR (Managed Detection and Response)	U11
12	Usługa SOC (Security Operation Center)	U12
13	Usługa CTI (Cyber Threat Intelligence)	U13
14	Usługa typu security awareness do symulowanych ataków socjotechnicznych	U14
15	Usługa ochrony AntyDDoS	U15
16	Usługa kopii zapasowych w chmurze obliczeniowej	U16

17	Usługa redundancji w chmurze obliczeniowej	U17
18	Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji	U18
19	Nadzór nad realizacją/wdrożeniem zaprojektowanego rozwiązania z zakresu bezpieczeństwa	U19
20	Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	U20
21	Utrzymanie, zarządzanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	U21
22	Audyt SZBI, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów, audyt (re)certyfikacji SZBI na zgodność z normami	U22
23	Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników	U23
24	Szkolenia z zakresu cyberbezpieczeństwa – szkolenia dla kadry istotnej z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji	U24
25	Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego	U25

26	Szkolenia z zakresu cyberbezpieczeństwa - 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	U26
27	Certyfikacja z zakresu cyberbezpieczeństwa: wyrobów (urządzeń i oprogramowania), usług i procesów, certyfikacja kompetencji (osób)	U27
28	Szkolenia przygotowujące do certyfikacji z zakresu cyberbezpieczeństwa.	U28

c) usługi wspomagające realizację Projektu grantowego, w szczególności usługi doradcze osób lub podmiotów zewnętrznych posiadających stosowne kwalifikacje i min. 2-letnie doświadczenie w prowadzeniu projektów IT zawierających komponent cyberbezpieczeństwa oraz stosowne certyfikaty lub równoważne poświadczenia (np. kwalifikację zawodową) potwierdzające możliwość wykonania zlecenia. Kwalifikowalność kosztów tylko w okresie realizacji Projektu grantowego;

d) szkolenia: zakup i organizacja szkoleń stacjonarnych lub/ i online dedykowanych dla pracowników zorganizowanych przez osoby lub 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 grantowego;

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

4. **Koszty pośrednie**: w ramach kategorii istnieje możliwość wskazania kwoty ryczałtowej **do 5% wartości** grantu. W ramach kategorii kosztów pośrednich istnieje możliwość rozliczenia kosztów administracyjnych, delegacji, wynagrodzenia kadry zarządzającej Projektem grantowym oraz wynagrodzeń osób zatrudnionych u Grantobiorcy i bezpośrednio zaangażowanych w Projekty grantowe (m.in. inżynier kontraktu, ekspert z dziedziny cyberbezpieczeństwa).

Katalog kosztów niekwalifikowalnych

1. Do wydatków niekwalifikowanych w ramach grantu zalicza się w szczególności wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa, w szczególności:
   - komputery stacjonarne i przenośne;
   - niezarządzalne urządzenia sieciowe;
   - wymiana i/lub doposażenie stacji roboczych z peryferiami;
   - akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki);
   - urządzenia mobilne (smartfony, tablety);
   - wymiana i/lub doposażenie serwerów dedykowanych do systemów dziedzinowych, niezwiązane z wdrożeniem rozwiązań bezpieczeństwa;
   - materiały eksploatacyjne;
   - oprogramowanie biurowe, oprogramowanie do elektronicznego zarządzania dokumentacją i oprogramowanie systemów operacyjnych, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;
   - szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;
   - usługi dostępu do internetu, abonamenty telefoniczne;
   - budowa infrastruktury sieci LAN/WAN/Radiowej/Światłowodowej;
   - rozwiązania w zakresie bezpieczeństwa fizycznego;
   - rozwiązania w zakresie ochrony informacji niejawnych;

- agregaty prądotwórcze;
- urządzenia typu UPS;
- akumulatory do urządzeń typu UPS.

Sposób rozliczenia grantu

1. W celu rozliczenia grantu, Grantobiorca składa do NASK-PIB Wniosek rozliczający, za pomocą udostępnionego narzędzia informatycznego, do którego załącza dokumentację finansową potwierdzająca 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.
2. Wraz z wnioskiem rozliczającym, Grantobiorca zobowiązany jest do przekazania formularza potwierdzającego realną propozycję zwiększenia odporności w wyniku realizacji Projektu grantowego. Ocena skuteczności zwiększenia odporności badana jest na podstawie danych wejściowych, wskazanych przez Grantobiorców na etapie składania Wniosku.
3. Na potwierdzenie ubezpieczenia sprzętu zostanie przedstawiona polisa obejmująca zadeklarowany w ubezpieczeniu sprzęt. W zakresie potwierdzenia prawidłowości wyboru dostawców i wykonawców - na żądanie CPPC lub NASK-PIB, Grantobiorca przedłoży dokumentację z postępowania o udzielenie zamówienia, zgodnie z Wytycznymi dotyczącymi kwalifikowalności wydatków na lata 2021-2027 lub ustawą z dnia 11 września 2019 r - Prawo zamówień publicznych.

ZASADY DOTYCZĄCE MONITOROWANIA I KONTROLI PROJEKTÓW GRANTOWYCH

Grantobiorca zobowiązany będzie do pomiaru wartości osiągniętych w wyniku realizacji Projektu grantowego, zamieszczonych we Wniosku. Za pomocą udostępnionego narzędzia informatycznego, w celu rozliczenia grantu, przekaże informacje o postępie rzeczowym oraz

finansowym. Szczegółowy sposób monitorowania i sprawozdawczości przedstawia Umowa o powierzenie grantu.

NASK-PIB przygotuje plan rozliczenia Grantobiorców oraz kontroli, w której wskaże listę Grantobiorców, w przypadku których dokona tej kontroli. Możliwe formy kontroli to kontrola zza biurka (pogłębiona weryfikacja w oparciu o dokumentację) oraz kontrola na miejscu realizacji Projektu.

ZASADY DOTYCZĄCE ODZYSKIWANIA GRANTÓW W PRZYPADKU ICH WYKORZYSTANIA NIEZGODNIE Z CELAMI PROJEKTU LUB NIEWYKORZYSTANIA

Umowa o powierzenie grantu określa sposób postępowania w przypadku stwierdzenia, że Projekt grantowy jest realizowany niezgodnie z umową. Umowa o powierzenie grantu określa również sposób zwrotu środków w przypadku nie osiągnięcia wskaźników na zakładanym poziomie.

MINIMALNY ZAKRES UMOWY O POWIERZENIE GRANTU

1. W ramach grantu kwalifikowalne są wydatki poniesione od 1.01.2025 r. do dnia zakończenia realizacji Projektu grantowego określonego w Porozumieniu, jednakże nie dłużej niż do 31.12.2026 r.
2. Projekt grantowy powinien trwać od dnia wejścia w życie Porozumienia o powierzenie grantu, jednak nie później niż do **31.12.2026 r.**
3. Grantobiorca jest zobowiązany do wydatkowania grantu zgodnie z przepisami obowiązującego prawa, w sposób oszczędny, racjonalny i efektywny w okresie realizacji Projektu grantowego i zgodnie z jego celami.
4. Grantobiorca dokonując zakupu środków trwałych, wartości niematerialnych i prawnych oraz usług wskazanych jako kwalifikowane w ramach Projektu

grantowego 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 80 tys. zł netto, tj. bez podatku od towarów i usług (VAT), jest zobligowany do stosowania bazy konkurencyjności dostępnej pod adresem **Baza konkurencyjności**.

5. Grantobiorca jest zobowiązany do utrzymania efektów Projektu grantowego, w tym do opracowania oraz wdrożenia procedury monitorowania w okresie trzech lat od zakończenia utrzymywania długoterminowych efektów Projektu grantowego tj. utrzymania środków trwałych i usług nabytych w ramach Projektu grantowego przez okres 3 lat od dnia zakończenia Projektu grantowego. Za zakończenie Projektu grantowego rozumie się zaakceptowanie przez NASK-PIB końcowego rozliczenia Projektu grantowego.

KONTAKT:

Wszelkie informacje pozyskają Państwo na stronie **Cyberbezpieczny Rząd**
Kontakt e-mail: **cyberbezpiecznyrzad@cppc.gov.pl**
Infolinia obsługiwaną przez NASK-PIB pod nr: +48 22 182 22 94
Odpowiedzi polegające na wyjaśnieniu procedur będą dodatkowo zamieszczane w pytaniach i odpowiedziach.