Regulamin Konkursu Grantowego pn.

“Cyberbezpieczny Rząd”

Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo

Cyberbezpieczeństwo - Cyberbezpieczny Rząd

Krajowy Plan Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności

§1 Słownik pojęć:

1. **KPO** – Krajowy Plan Odbudowy i Zwiększania Odporności, zatwierdzony Decyzją wykonawczą Rady (UE) z dnia 17 czerwca 2022 r. w sprawie zatwierdzenia oceny planu odbudowy i zwiększania odporności Polski (COM(2022)268 final), będący planem rozwojowym w rozumieniu Ustawy;
2. **Efekty długoterminowe Projektu grantowego** - zachowanie efektów Projektu w okresie przekraczającym ramy czasowe obowiązywania Instrumentu na rzecz Odbudowy i Zwiększania Odporności i nie mających charakteru powtarzających się krajowych wydatków budżetowych, oraz zobowiązanie do niepoddawania Przedsięwzięcia znaczącym modyfikacjom, tj. zmianie własności elementu infrastruktury, która daje przedsiębiorstwu lub podmiotowi publicznemu nienależną korzyść lub istotnej zmianie wpływającej na charakter operacji, jej cele lub warunki wdrażania, mogącej doprowadzić do naruszenia pierwotnych celów operacji;
3. **Grant** – środki finansowe, które Partner przekaże Grantobiorcy na podstawie Umowy/Porozumienia na realizację zadań służących osiągnięciu celu Przedsięwzięcia grantowego;
4. **Grantobiorca** – urząd obsługujący centralne lub naczelne organy administracji rządowej lub urząd wojewódzki, podmioty inne niż Ostateczny Odbiorca Wsparcia Przedsięwzięcia grantowego albo Partner przedsięwzięcia, wybrany w niniejszym naborze;
5. **Ostateczny Odbiorca Wsparcia –** Centrum Projektów Polska Cyfrowa (dalej jako CPPC lub OOW);
6. **Inwestycja** – oznacza to inwestycję w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/241 z dnia 12 lutego 2021 r. ustanawiającego Instrument na rzecz Odbudowy i Zwiększania Odporności (Rozporządzenie 2021/241) zmierzającą do osiągnięcia celu w Planie rozwojowym; C3.1.1 inwestycja w rozumieniu Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/241 z dnia 12 lutego 2021 r. ustanawiające Instrument na rzecz Odbudowy i Zwiększania Odporności (rozporządzenia RRF) zmierzająca do osiągnięcia celu w planie rozwojowym, pn. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo;
7. **Jednostka podległa -** jednostka budżetowa w rozumieniu art. 9 pkt 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2024 r. poz. 1530 ze zm.), podlegająca w

sposób administracyjny lub finansowy naczelnemu lub centralnemu organowi administracji rządowej lub wojewodom;

8. **Komisja Przyznająca Granty** – komisja zatwierdzająca listę rankingową Wniosków w formie Grantu według zasad określonych w niniejszym Regulaminie (dalej Komisja lub KPG);
9. **Konkurs Grantowy** – nabór, o którym mowa w niniejszym Regulaminie, prowadzony przez OOW w celu wyłonienia Grantobiorców (dalej Konkurs lub Nabór);
10. **LSI** – aplikacja służąca do kompleksowej obsługi Wniosków o przyznanie Grantu (w zakresie składania Wniosków, oceny Wniosków, komunikacji między Partnerem a Wnioskodawcą grantu), dostępna na stronie internetowej Przedsięwzięcia oraz na stronie https://lsi.cppc.gov.pl/beneficjent;
11. **Partner** – Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB);
12. **Projekt grantowy** - przedsięwzięcie realizowane przez Grantobiorcę, zmierzające do osiągnięcia założonego celu określonego wskaźnikami, z określonym budżetem, początkiem i końcem realizacji. Nie jest to projekt w rozumieniu funduszy strukturalnych, Funduszu Spójności albo Funduszu na rzecz Sprawiedliwej Transformacji, zwany dalej „Projektem".
13. **Przedsięwzięcie** lub **Przedsięwzięcie grantowe** – Przedsięwzięcie pn. "Cyberbezpieczny Rząd" „Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)." realizowane w ramach KPO, inwestycji C3.1.1. przez CPPC i NASK-PIB;
14. **Regulamin Konkursu Grantowego lub Regulamin** – niniejszy Regulamin;
15. **Strona internetowa Przedsięwzięcia** – https://www.gov.pl/web/cppc/inwestycja-c-311-konkurs-grantowy-cyberbezpieczny-rzad
16. **SZOP** – Szczegółowy Opis Priorytetów Programu Krajowy Plan Odbudowy i Zwiększania Odporności;
17. **Umowa/Porozumienie** lub **Umowa/Porozumienie o powierzenie grantu** – umowa/porozumienie zawarta/zawarte pomiędzy Grantobiorcą i OOW określająca w szczególności zakres Projektu Grantowego, zadania Grantobiorcy objęte Grantem, kwotę Grantu, okres realizacji Umowy/Porozumienia, warunki przekazania i rozliczenia Grantu;

18. **Ustawa –** ustawa z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz.U. 2024 r. poz. 324 ze zm.)**;**
19. **Wniosek o przyznanie grantu lub Wniosek** – wniosek złożony przez podmiot uprawniony w celu uzyskania Grantu (którego wzór stanowi Załącznik nr 1) złożony za pośrednictwem aplikacji do składania wniosków**, tj. LSI;**
20. **Wnioskodawca grantu** – podmiot krajowego systemu cyberbezpieczeństwa (KSC) taki jak: urząd obsługujący centralny lub naczelny organ administracji rządowej lub urząd wojewódzki, aplikujący o Grant na realizację Projektu grantowego, uprawniony do złożenia Wniosku za pomocą LSI;
21. **Wskaźniki przedsięwzięcia** – wskaźniki, których opis stanowi Załącznik nr 7 do Regulaminu Konkursu Grantowego;
22. **Wydatki faktycznie poniesione** – wydatki poniesione w znaczeniu kasowym, tj. jako rozchód środków pieniężnych z kasy lub rachunku płatniczego.

§2 Podstawy prawne

1. Konkurs Grantowy jest organizowany w oparciu o następujące akty prawne:
    1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/241 z dnia 12 lutego 2021 r. ustanawiające Instrument na rzecz Odbudowy i Zwiększania Odporności, (Dz. Urz. UE L 57 z 18.02.2021, s. 17);
    2) Ustawę;
    3) Decyzję wykonawczą Rady w sprawie zatwierdzenia oceny planu odbudowy i zwiększania odporności Polski (COM(2022) 268 final), przyjętą w dniu 17 czerwca 2022 r.;
    4) Ustawę z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725);
    5) Decyzję z dnia 13.02.2025 r. nr KPOD.05.10-IW.06-0001/25-00 o objęciu Przedsięwzięcia wsparciem pn. „Cyberbezpieczny Rząd”
    6) Umowę o Partnerstwie z dnia 13 stycznia 2025 r. zawartą przez OOW i Partnera, 7) Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 ze zm.).

§3 Informacje ogólne

1. Celem Przedsięwzięcia grantowego jest poprawa cyberbezpieczeństwa dla określonej grupy podmiotów krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz.1077 ze zm.) poprzez udzielenie im grantów.
2. Nabór realizowany jest przez OOW we współpracy z Partnerem.
3. Celem naboru jest wybór Projektów grantowych, które poprzez realizację w największym stopniu przyczynią się do osiągniecia celu szczegółowego C3.1.1. „Infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo" w ramach KPO. Cel ten będzie realizowany poprzez Przedsięwzięcie grantowe.
4. Przedmiotem naboru jest wybór Grantobiorców, którzy będą realizować Projekty grantowe mające na celu osiągnięcie Wskaźników w zakresie i terminach określonych w Regulaminie.
5. Cel Przedsięwzięcia wpisuje się zarówno w cele KPO, jak i cele określone w SZOP.
6. OOW przyzna Grantobiorcy Grant na zadania w ramach poniżej wskazanych obszarów:
    1) **Obszar Organizacji** - środki można przeznaczyć na następujące działania (usługi):
        a) przegląd, aktualizacja lub opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji,
        b) wprowadzenie środków obejmujących m.in.: politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługę incydentu, ciągłość działania i zarządzanie kryzysowe, polityki i procedury stosowania kryptografii i szyfrowania, politykę kontroli dostępu, stosowanie uwierzytelniania wieloskładnikowego,
        c) audyt systemu zarządzania bezpieczeństwem informacji przeprowadzonego przez wykwalifikowanego audytora, stanowiący dowód wdrożenia i stosowania ww. systemu w organizacji lub instytucji.
    2) **Obszar Kompetencji** - środki można przeznaczyć na następujące działania (usługi):
        a) szkolenia z zakresu cyberbezpieczeństwa dla kadry podmiotu KSC istotnej z punktu widzenia wdrożonej polityki cyberbezpieczeństwa lub systemu zarządzania bezpieczeństwem informacji, w tym w szczególności w zakresie środków wdrażanych w ramach Projektu grantowego,

b) szkolenia z zakresu cyberbezpieczeństwa dla: specjalistów odpowiedzialnych za bezpieczeństwo teleinformatyczne, kadry kierowniczej oraz pozostałych pracowników podmiotu KSC, obejmujących m.in. symulowane cyberataki na użytkowników sieci i systemów informacyjnych w organizacji (np. phishing).

3) **Obszar Technologii** - 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.

7. Niniejszy Regulamin określa zasady naboru i sposób wyboru Grantobiorców w ramach Konkursu Grantowego.
8. Konkurs Grantowy jest prowadzony na terenie całej Polski.
9. Grantobiorcy będą realizowali Projekty grantowe na podstawie Umowy/Porozumienia, zawartej pomiędzy Grantobiorcą a OOW.
10. Warunki dotyczące okresu realizacji Projektów grantowych:

1) okres realizacji Projektów grantowych trwa od dnia wejścia w życie Umowy/Porozumienia do **31.12.2026 r.;**

2) dopuszcza się kwalifikowalność wydatków poniesionych w okresie **od 01.01.2025 r**. do dnia zakończenia realizacji Projektu grantowego określonego w Umowie/Porozumieniu, jednakże nie dłużej niż do 31.12.2026 r.

11. Wniosek uznaje się za złożony, jeśli spełnia następujące warunki:
    1) został złożony w terminie, o którym mowa w § 5 ust. 1 pkt 2.
    2) został złożony zgodnie z zasadami określonymi w § 5 ust. 2.

§4 Podmioty uprawnione do udziału w Konkursie Grantowym i zasady finansowania Projektów grantowych

1. Do udziału w Konkursie Grantowym uprawnione są podmioty, o których mowa w art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 ze zm.), które są urzędami obsługującymi centralne lub naczelne organy administracji rządowej i wojewodów (podmioty wymienione na liście w Załączniku nr 2, lista nie stanowi katalogu zamkniętego). Wsparciem mogą być objęte również jednostki podległe centralnym lub naczelnym organom administracji rządowej lub wojewodom.
2. Alokacja na Granty w Konkursie Grantowym pn. "Cyberbezpieczny Rząd" wynosi **350 000 000,00 PLN netto.**
3. Wysokość przyznanego Grantu dla Projektu grantowego wynosi **100% kosztów kwalifikowalnych**.
4. Minimalna wysokość Grantu dla Grantobiorcy wynosi **500 000,00 PLN netto**, natomiast maksymalna wysokość Grantu wynosi **10 000 000,00 PLN netto**. Wysokość Grantu dla jednego Grantobiorcy uzależniona jest od wskazanej liczby jednostek mu podległych.
5. Wnioskodawca grantu, który wskazał wsparcie **do 4 (czterech) jednostek podległych włącznie**, może ubiegać się o grant wysokości **do 5 000 000,00 PLN netto.** Wnioskodawca grantu, który wskazał wsparcie **5 (pięciu) lub więcej jednostek podległych**, może ubiegać się o grant w wysokości **do 10 000 000,00 PLN netto.**
6. Jeżeli wniosek obejmuje wsparciem również jednostki podległe centralnym lub naczelnym organom administracji rządowej lub wojewodom – Grantobiorca zobowiązany jest zapewnić przejrzyste zasady nieodpłatnego udostępniania/przekazywania środków trwałych, wartości materialnych i prawnych lub usług i w razie potrzeby, uwzględnić przyjęty przez siebie sposób postępowania w tym zakresie w odniesieniu do udzielania zamówień w ramach Projektu grantowego (szacowanie wartości zamówienia, opis przedmiotu zamówienia, projektowane postanowienia umowne).

7. **Wydatki poniesione przez Grantobiorcę na podatek VAT ze środków Grantu będą uznane za niekwalifikowalne. Podatek VAT jest finansowany ze środków własnych Grantobiorcy.**
8. Do wydatków kwalifikowalnych w ramach Grantu zalicza się w szczególności:

   1) **środki trwałe/dostawy** (np. 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 802.1X (switch)	S27
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** 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:

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 do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu bezpieczeństwa	O45

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

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

b) usługi informatyczne i szkolenia zwiększające poziom bezpieczeństwa informacji, tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach teleinformatycznych;

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;

d) szkolenia: zakup i organizacja szkoleń stacjonarnych (z wyłączeniem kosztów noclegu i dojazdu) lub/ i online dedykowanych dla pracowników zorganizowanych przez osoby lub podmioty posiadające stosowną wiedzę oraz min. 2-letnie doświadczenie w przygotowaniu
i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń;

Wykaz usług obszarów organizacji, kompetencji i technologii wskazane w pkt. 3 lit. a-d:

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 sandbox do badania bezpieczeństwa aplikacji oraz plików	U05
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 z zakresu 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
29	Materiały promocyjne i informacyjne (drukowane i elektroniczne) upowszechniające wśród pracowników świadomość o cyberzagrożeniach i cyberbezpieczeństwie, np.: newsletter, periodyk o cyberhigienie, materiały budujące i wzmacniające świadomość o zagrożeniach w cyberprzestrzeni.	U29

9. Kwalifikowalne będą tylko koszty poniesione w okresie realizacji Przedsięwzięcia grantowego. Koszty usług np. gwarancji, licencji, ubezpieczenia wykraczające poza okres kwalifikowalności będą kwalifikowalne proporcjonalnie w czasie trwania okresu kwalifikowalności.
10. **Koszty pośrednie**: w ramach kategorii istnieje możliwość wskazania kwoty ryczałtowej **do 5% wartości** Grantu. W ramach kategorii kosztów pośrednich istnieje możliwość rozliczenia m.in. kosztów administracyjnych, delegacji, wynagrodzenia kadry zarządzającej Projektem grantowym oraz wynagrodzeń osób zatrudnionych u Grantobiorcy i bezpośrednio zaangażowanych w Projekt grantowy (m.in. inżynier kontraktu, ekspert z dziedziny cyberbezpieczeństwa).
11. Koszty kwalifikowalne w ramach kosztów pośrednich oraz kosztów bezpośrednich muszą być rozdzielone i jednoznacznie przypisane do odpowiednich kategorii. Niedopuszczalne jest podwójne finansowanie tych samych wydatków, tj. koszty ujęte w kategorii kosztów pośrednich nie mogą być jednocześnie finansowane jako koszty bezpośrednie, a koszty

zakwalifikowane jako bezpośrednie nie mogą być uwzględnione w kosztach pośrednich. W przypadku stwierdzenia naruszenia tej zasady, wydatki te zostaną uznane za niekwalifikowalne i podlegać będą zwrotowi.

12. Do **wydatków niekwalifikowanych** w ramach Grantu zalicza się w szczególności wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa, w szczególności:

a) komputery stacjonarne i przenośne;
b) niezarządzalne urządzenia sieciowe;
c) wymiana i/lub doposażenie stacji roboczych z peryferiami;
d) akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki);
e) urządzenia mobilne (smartfony, tablety);
f) wymiana i/lub doposażenie serwerów dedykowanych do systemów dziedzinowych, niezwiązane z wdrożeniem rozwiązań bezpieczeństwa;
g) materiały eksploatacyjne;
h) oprogramowanie biurowe, oprogramowanie do elektronicznego zarządzania dokumentacją i oprogramowanie systemów operacyjnych, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;
i) szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;
j) usługi dostępu do internetu, abonamenty telefoniczne;
k) budowa infrastruktury sieci LAN/WAN/radiowej/światłowodowej;
l) rozwiązania w zakresie bezpieczeństwa fizycznego;
m) rozwiązania w zakresie ochrony informacji niejawnych;
n) agregaty prądotwórcze;
o) urządzenia typu UPS;
p) akumulatory do urządzeń typu UPS.

§5 Zasady i sposób wyboru Wniosków

1. **Nabór Wniosków:**

1) Wnioski zostaną wybrane w otwartym naborze, z zachowaniem zasady bezstronności i przejrzystości.
2) Nabór Wniosków trwać będzie od **28.02.2025 r.** do **31.03.2025 r**. do godziny 16:00. W uzasadnionych przypadkach nabór może zostać wydłużony. OOW zastrzega, w razie powstania oszczędności, możliwość przeprowadzenia naboru uzupełniającego.
3) Wszelkie zmiany terminu trwania naboru będą publikowane na stronie internetowej Przedsięwzięcia wraz ze wskazaniem terminów składania Wniosków.

2. **Sposób składania Wniosków:**
   1) Wzór Wniosku jest dostępny na stronie internetowej Przedsięwzięcia oraz stanowi Załącznik nr 1 do Regulaminu. Wnioskodawca grantowy zobowiązany jest do zapoznania się i stosowania Instrukcji, dostępnej pod adresem Instrukcje użytkownika systemu LSI - Centrum Projektów Polska Cyfrowa - Portal Gov.pl Wnioskodawca grantu może dokonać samodzielnej zmiany kontekstu, a w uzasadnionych przypadkach, może zwrócić się z prośbą do OOW o zmianę tego kontekstu (zmiana kontekstu opisana jest w Instrukcji) dla konta w systemie LSI nie później niż 7 dni przed planowanym zakończeniem naboru do Konkursu Grantowego.
   2) Wniosek należy wypełnić za pomocą systemu LSI.
   3) Złożenie Wniosku oznacza, że Wnioskodawca zapoznał się z Regulaminem Konkursu Grantowego wraz Załącznikami i akceptuje ich zasady.
   4) Wnioskodawca grantu ma możliwość wycofania Wniosku przesyłając za pośrednictwem LSI pismo z informacją o wycofaniu z Konkursu Grantowego, podpisane elektronicznie zgodnie z reprezentacją Wnioskodawcy grantu.
   5) Wnioskodawca grantu uprawniony jest do złożenia jednego Wniosku w Konkursie Grantowym. W przypadku złożenia większej liczby Wniosków, oceniany będzie ten złożony jako pierwszy.
   6) Wniosek powinien być złożony przez Wnioskodawcę grantu i podpisany przez osobę upoważnioną do reprezentacji Wnioskodawcy. Do Wniosku należy dołączyć dokumenty potwierdzające umocowanie do reprezentowania Wnioskodawcy grantu.

3. **Sposób i zasady oceny Wniosków:**
   1) O przyznaniu Grantu w naborze i w naborze uzupełniającym decyduje wynik oceny Wniosku.
   2) Ocena Wniosku będzie dokonywana przez Komisję Przyznającą Granty, na podstawie ocen cząstkowych realizowanych przez ekspertów na etapie oceny formalnej i

merytorycznej w systemie LSI. KPG będzie działała na podstawie odrębnego Regulaminu prac Komisji.

3) W skład Komisji wchodzą pracownicy Partnera, co najmniej: Przewodniczący i Sekretarz.
4) Wnioski zostaną poddane ocenie formalnej i merytorycznej w oparciu o kryteria wyboru Projektów grantowych, określonych w Załączniku nr 3 do Regulaminu.
5) W zakresie oceny formalnej zostanie zweryfikowane, czy Wnioskodawca grantu i Wniosek spełniają zdefiniowane kryteria oceny formalnej.
6) Kryteria formalne mają charakter zero - jedynkowy (zasada: nie spełnia - 0; spełnia - 1).
7) Aby Wniosek uzyskał pozytywny wynik z oceny formalnej i był przekazany do oceny merytorycznej, musi spełnić wszystkie kryteria w ocenie formalnej.
8) W przypadku stwierdzenia uchybień lub braków formalnych we Wniosku, Wnioskodawca grantu zostanie jednokrotnie wezwany do ich poprawy lub uzupełnień, przy czym wezwanie to będzie stanowiło jedyną możliwość uzupełnienia lub skorygowania uchybień lub braków formalnych Wniosku.
9) Wezwanie do uzupełnienia lub poprawy Wniosku zostanie przekazane Wnioskodawcy grantu za pomocą LSI.
10) Wnioskodawca grantu będzie miał 5 dni kalendarzowych od dnia otrzymania wezwania na dokonanie niezbędnych poprawek i ponowne złożenie wniosku.
11) Poprawiony Wniosek należy przesłać zgodnie z instrukcją zawartą w wezwaniu, zachowując wymogi formalne określone w Regulaminie.
12) Niezłożenie poprawionego Wniosku w wyznaczonym terminie skutkować będzie oceną jego pierwotnej wersji.
13) W zakresie oceny merytorycznej zostanie zweryfikowane czy Wniosek w części merytorycznej spełnia zdefiniowane kryteria oceny merytorycznej stanowiące Załącznik nr 3 do niniejszego regulaminu.
14) Kryteria merytoryczne nr 1, 2, 3 mają charakter zero - jedynkowy (zasada: nie spełnia - 0; spełnia - 1). Wniosek musi spełniać każde z tych kryteriów.
15) W zakresie kryterium merytorycznego nr 4. Ocena planowanego zakresu postępu Projektu grantowego zostanie przyznana pula punktów odpowiadająca deklarowanemu przyrostowi odporności na cyberzagrożenia. Im większa liczba uzyskanych punktów, tym wyższa ocena kryterium merytorycznego.

16) Przyrost odporności na cyberzagrożeniażenia jest obliczany jako różnica wartości sumy punktów planowanego i obecnego poziomu wszystkich rozwiązań bezpieczeństwa.

17) Rozwiązania bezpieczeństwa w ramach prowadzonych Projektów grantowych powinny dotyczyć zwartych w poniższej tabeli obszarów:

L.p.	Obszary	Rozwiązanie
1	Organizacyjny	Opracowanie, wdrożenie SZBI
2	Kompetencyjny	Szkolenia z zakresu cyberbezpieczeństwa
3	Techniczny	Bezpieczeństwo systemów informatycznych
4	Techniczny	Bezpieczeństwo www (stron i/lub platform internetowych)
5	Techniczny	Bezpieczeństwo stacji roboczych
6	Techniczny	Rozwiązanie bezpieczeństwa sieci
7	Techniczny	Rozwiązania bezpieczeństwa styku sieci internet z usługami wewnętrznymi
8	Techniczny	Zwiększenie niezawodności i wydajności
9	Techniczny	Rozwiązania sieciowe WAN/LAN/WIFI
10	Techniczny	Rozwiązania wirtualizacyjne
11	Techniczny	Rozwiązania kopii zapasowych
12	Techniczny	Redundancja (HA)
13	Techniczny	Rozwiązania zarządzania operacyjnego
14	Techniczny	Bezpieczeństwo komunikacji
15	Techniczny	Monitorowanie bezpieczeństwa
16	Techniczny	Reagowanie w zakresie bezpieczeństwa
17	Techniczny	Zarządzanie uprawnieniami użytkowników
18	Techniczny	Zabezpieczanie dowodów cyfrowych

18) Wniosek w części dotyczącej kryterium 4. Ocena planowanego postępu realizacji Projektu grantowego obejmuje analizę zbioru pozycji kosztów kwalifikowanych,

uporządkowanych w ramach określonych rozwiązań bezpieczeństwa. Ocenie podlega zarówno obecny, jak i przewidywany zakres i poziom ich wdrożenia.

19) We Wniosku Wnioskodawca grantu dla każdego stosowanego obecnie i planowanego rozwiązania bezpieczeństwa wskazuje produkty, działania i usługi bezpieczeństwa, przedstawia jego charakterystykę i opis oraz dokonuje oceny zakresu i poziomu jego wdrożenia.

20) Wskazanie obecnie wdrożonych i planowanych do wdrożenia produktów, działań i usług bezpieczeństwa, dla każdego z rozwiązań bezpieczeństwa, jest realizowane poprzez:
    a) zaznaczenie wyboru z predefiniowanej listy pozycji najczęściej stosowanych w realizacji danego rozwiązania bezpieczeństwa;
    b) dodanie innych pozycji ze zbioru pozycji kosztów kwalifikowalnych;
    c) dodanie innych pozycji spoza zbioru pozycji kosztów kwalifikowalnych, przy czym pozycje te muszą należeć do rozwiązań zdefiniowanych dla obszarów organizacji kompetencji i technologii.

21) Każde rozwiązanie bezpieczeństwa oceniane jest, dla stanu obecnego, w skali punktowej z przedziału (0-3), a dla stanu planowanego, w skali punktowej z przedziału (ND, 0-3), gdzie poszczególne wartości reprezentują zakres i poziom rozwiązań bezpieczeństwa, które należy rozumieć odpowiednio jako:
    a) ND – nie dotyczy: nie wnioskuje się o sfinansowanie danego rozwiązania obszarowego bezpieczeństwa;
    b) 0 – brak rozwiązania obszarowego bezpieczeństwa: nie zakupione żadne produkty, usługi lub rozwiązania bezpieczeństwa lub zakupione pojedyncze produkty (oprogramowanie lub sprzęt) ale nie wdrożone;
    c) 1 – niski zakres i poziom rozwiązania obszarowego bezpieczeństwa: zakupione i wdrożone pojedyncze produkty (oprogramowanie lub sprzęt) lub usługi, wdrożone w minimalnym lub małym zakresie funkcjonalnym, zapewniające niski poziom bezpieczeństwa, pokrywające w minimalnym lub małym stopniu dany obszar bezpieczeństwa, eksploatowane i utrzymywane z niska atencją, sporadycznie i nieregularnie aktualizowane;
    d) 2 – średni zakres i poziom rozwiązania obszarowego bezpieczeństwa: zakupione i wdrożone zestawy zintegrowanych produktów (oprogramowanie lub sprzęt) lub usług jako spójne rozwiązanie, wdrożone w średnim zakresie funkcjonalnym,

zapewniające średni poziom bezpieczeństwa, pokrywające w średnim stopniu dany obszar bezpieczeństwa, eksploatowane i utrzymywane ze średnią atencją, wyniki uzyskanego poziomu bezpieczeństwa analizowane i uwzględniane w aktualizacji konfiguracji produktów rozwiązania, regularnie aktualizowane;

e) 3 – wysoki zakres i poziom rozwiązania obszarowego bezpieczeństwa: zakupione i wdrożone zestawy zintegrowanych produktów (oprogramowanie lub sprzęt) lub usług jako spójne rozwiązanie, wdrożone w wysokim/pełnym zakresie funkcjonalnym, zapewniające wysoki poziom bezpieczeństwa, pokrywające w wysokim stopniu dany obszar bezpieczeństwa, eksploatowane, utrzymywane i zarządzane z wysoką atencją, wyniki uzyskanego poziomu bezpieczeństwa analizowane i uwzględniane w aktualizacji konfiguracji produktów rozwiązania i architektury rozwiązania, regularnie aktualizowane.

22) Procedura oceny obecnych i planowanych do wdrożenia rozwiązań bezpieczeństwa jest następująca:

1) dla każdego obecnego rozwiązania bezpieczeństwa:

a) wskazać z predefiniowanej listy produktów, działań i usług te, które są aktualnie wdrożone i stosowane, poprzez wybór z listy opcji pozycji T (tak) lub N (nie).

b) w przypadku stosowania produktów, działań i usług innych niż predefiniowane, wprowadzić poprzez wybór z list kosztów kwalifikowanych i/lub poprzez wprowadzenie pozycji spoza listy kosztów kwalifikowanych funkcjami interaktywnymi Wniosku.

c) scharakteryzować i opisać rozwiązania bezpieczeństwa (krótko, ok. 200-250 znaków).

d) ocenić zakres i poziom rozwiązania bezpieczeństwa w skali punktowej z przedziału (0-3), zgodnie z zasadami, poprzez wybór z listy opcji pozycji (0,1,2,3).

2) dla każdego planowanego rozwiązania bezpieczeństwa:

a) wskazać z predefiniowanej listy produktów, działań i usług te, które mają stanowić ich docelowe elementy składowe, poprzez wybór z listy opcji pozycji T (tak) lub N (nie).

b) w przypadku planowania do wdrożenia produktów, działań i usług innych niż predefiniowane, wprowadzić poprzez wybór z

list kosztów kwalifikowanych i/lub poprzez wprowadzenie pozycji spoza listy kosztów kwalifikowanych funkcjami interaktywnymi wniosku.

c) jeśli dotyczy - scharakteryzować i opisać rozwiązania bezpieczeństwa (krótko, ok. 200-250 znaków). Jeśli nie dotyczy: opis nie jest wymagany.

d) ocenić zakres i poziom rozwiązania bezpieczeństwa w skali punktowej z przedziału (ND,0-3), zgodnie z zasadami, poprzez wybór z listy opcji pozycji (ND,0,1,2,3).

23) Premiowane są rozwiązania bezpieczeństwa uznane za podnoszące w największym stopniu odporność i mitygujące w największym stopniu aktualnie cyberzagrożenia, tj. Szkolenia z zakresu cyberbezpieczeństwa (poz. 2), Rozwiązanie bezpieczeństwa sieci (poz. 6), Rozwiązania bezpieczeństwa styku sieci internet z usługami wewnętrznymi (poz. 7), Monitorowanie bezpieczeństwa (poz.15), Zarządzanie uprawnieniami użytkowników (poz. 17). Wskazana we Wniosku ocena stanu planowanego dla tych rozwiązań bezpieczeństwa uzyskuje mnożnik *1,5 (jest powiększana o 50%) w ramach oceny kryterium merytorycznego.

24) Ocena Wniosków jest realizowana na podstawie liczby uzyskanych punktów dla deklarowanego planowanego przyrostu, o którym mowa w ust. 17, zakresu i poziomu rozwiązań bezpieczeństwa. Im większa liczba uzyskanych punktów, tym wyższa ocena rankingowa i wyższa pozycja na liście rankingowej, w kolejności od najwyższej do najniższej.

25) W przypadku, gdy co najmniej dwa Wnioski uzyskały taką samą liczbę punktów na liście rankingowej, a pozostałe do rozdysponowania środki są niewystarczające dla objęcia wsparciem każdego z tych Projektów grantowych w pełnej wysokości, grant otrzyma ten Wnioskodawca grantu, który złożył Wniosek wcześniej.

26) Wynik oceny jest ostateczny i nie podlega procedurze odwoławczej. Wnioskodawca nie ma możliwości złożenia odwołania, zażalenia ani innych środków prawnych w celu zakwestionowania wyników oceny.

27) OOW publikuje listę rankingową oceny Wniosków, na stronie internetowej Przedsięwzięcia grantowego.

28) Informacja o zakończeniu oceny zostanie wysłana przez LSI do Wnioskodawców grantu.

29) Informacja o przyznaniu Grantu wskazuje wysokość przyznanych środków finansowych na realizację Projektu grantowego oraz liczbę punktów uzyskanych przez Wnioskodawcę grantu.
30) Informacja o odmowie przyznania Grantu wskazuje przyczyny nieprzyznania środków finansowych, w tym, w zależności od okoliczności, informację o wystąpieniu wad formalnych, niespełnieniu poszczególnych kryteriów, liczbie punktów uzyskanych przez Wnioskodawcę grantu.
31) Ocena Wniosków trwa 30 dni kalendarzowych liczonych od dnia zakończenia naboru.
32) Po wstępnej walidacji Wniosku możliwe będzie naniesienie poprawek przez Wnioskodawcę grantu zgodnie z uwagami KPG.
33) W przypadku stwierdzenia oczywistych omyłek lub braków we Wniosku uniemożliwiających przeprowadzenie oceny merytorycznej, w tym uwzględnienia w nim wydatków niezgodnych z zakresem kosztów kwalifikowalnych zgodnie z postanowieniami § 4 ust. 8 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 zostanie jednokrotnie wezwany do ich poprawy, przy czym wezwanie to będzie stanowiło jedyną możliwość uzupełnienia lub skorygowania braków merytorycznych. Wnioskodawca grantu będzie miał 5 dni kalendarzowych od dnia otrzymania wezwania na usunięcie oczywistej omyłki, uzupełnienie braków lub modyfikację zaplanowanych kosztów i/lub pozycji i opisów rozwiązań bezpieczeństwa.
34) W przypadku braku modyfikacji zaplanowanych kosztów i/lub pozycji i opisów rozwiązań bezpieczeństwa, 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.
35) W przypadku, gdy we Wniosku przyznanie Grantu została określona pozycja niekwalifikująca się do sfinansowania, następuje usunięcie całej pozycji kosztowej. Jeżeli we Wniosku o wsparcie w formie Grantu wskazano grupę kosztów niekwalifikujących się do sfinansowania w ramach danego obszaru zgodnie z § 4 ust. 10 i 12 wartość kwoty grantu obniżana jest o 10% w ramach danego obszaru.

36) W przypadku, gdy Wnioskodawca grantu nie zgadza się z decyzją KPG w zakresie kwalifikowalności wydatków i obniżenia wartości kwoty grantu 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 przyznanego Grantu.
37) 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 pierwotnie Wniosek o przyznanie Grantu;
38) Jeśli termin na poprawę lub uzupełnienie Wniosku o przyznanie Grantu przypada na dzień wolny od pracy (sobota, niedziela, święto), poprawa lub uzupełnienie powinna nastąpić nie później niż w dniu poprzedzającym.
39) W przypadku stwierdzenia omyłek lub braków we Wniosku o przyznanie Grantu, które nie uniemożliwiają dokonanie oceny Wniosku o przyznanie Grantu, dopuszcza się skorygowanie stwierdzonych błędów przy zawarciu Umowy/Porozumienia.
40) Fakt, że dany Projekt grantowy został zakwalifikowany do otrzymania grantu nie oznacza, że wszystkie koszty poniesione podczas jej realizacji będą uznane za kwalifikowalne. Grantobiorca ponosi pełną i wyłączną odpowiedzialność za roszczenia, straty, kary, opóźnienia i inne konsekwencje, które mogą wyniknąć z ponoszenia kosztów, które zostały uznane za niekwalifikowalne, pomimo uznania na etapie oceny Wniosku kosztu za kwalifikowalny. Grantobiorca ponosi także ryzyko za skutki niewłaściwego zarządzania i udokumentowania poniesionych wydatków w ramach realizacji Grantu. OOW nie ponosi odpowiedzialności za jakiekolwiek roszczenia, które mogą wyniknąć z realizacji Projektu grantowego, a które pozostają wyłącznie po stronie Grantobiorcy.

1. Prawdziwość oświadczeń i danych zawartych we Wniosku może zostać zweryfikowana w trakcie weryfikacji warunków formalnych i oceny, jak również przed i po zawarciu Umowy/Porozumienia.
2. Wnioskodawca grantu ma prawo dostępu do dokumentów związanych z oceną złożonego przez siebie Wniosku, z zastrzeżeniem, że dane osobowe członków KPG dokonujących oceny nie podlegają ujawnieniu.
3. Projekt grantowy może być oceniony pozytywnie, jeżeli jednocześnie:

2) spełniło kryteria wyboru Projektów grantowych i uzyskało wymaganą liczbę punktów;
3) Wnioskodawca grantu nie został wykluczony z możliwości otrzymania Grantu na podstawie przepisów odrębnych.

4. 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 przyznaniu Grantu.

4. **Sposób rozliczenia Grantu:**

1. W celu rozliczenia Grantu, Grantobiorca składa do OOW wniosek rozliczający za pośrednictwem aplikacji udostępnionej Grantobiorcy, do którego załącza faktury (np. 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 OOW, Grantobiorca przedłoży dokumentację z postępowania o udzielenie zamówienia, przeprowadzonego zgodnie z Zasadami kwalifikowania wydatków w Przedsięwzięciach realizowanych w ramach Inwestycji C3.1.1. Krajowego Planu Odbudowy i Zwiększania Odporności lub ustawą z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz.U. z 2024 r. poz. 1320).
2. Grantobiorca ma obowiązek dostarczenia wraz z wnioskiem rozliczającym Projektu grantowego informacji o wdrożonych produktach, działaniach i usługach bezpieczeństwa w ramach każdego z wnioskowanych i planowanych do wdrożenia rozwiązań bezpieczeństwa wraz z oceną uzyskanego ich zakresu i poziomu.
3. Grantobiorca przedstawia informacje, o których mowa w ust. 2 poprzez złożenie wniosku rozliczającego (za pomocą systemu służącego do rozliczania wniosków, dostępnego na stronie internetowej Przedsięwzięcia) i podając informacje o faktycznie wdrożonych produktach, działaniach i usługach bezpieczeństwa w ramach każdego z rozwiązań bezpieczeństwa wraz z oceną uzyskanego ich zakresu i poziomu, w miejsce planowanych do wdrożenia.

4. Sposób wypełniania Wniosku rozliczającego i zasady oceny dla etapu rozliczania są analogiczne jak dla etapu wnioskowania.
5. Grantobiorca w ramach realizacji Projektu grantowego zobowiązany jest do realizacji Wskaźników zgodnie z Załącznikiem nr 7 do Regulaminu.
6. Grantobiorca może wnioskować o zmianę zakresu Projektu grantowego na etapie jego realizacji, w szczególności w przypadku wystąpienia oszczędności w budżecie Projektu grantowego. Zmiana ta może dotyczyć zmian w harmonogramie, zakresie rzeczowym lub finansowym Projektu grantowego, pod warunkiem, że nie wpływa ona negatywnie na osiągnięcie zakładanych celów i Wskaźników oraz pozostaje zgodna z zasadami kwalifikowalności wydatków określonymi w Regulaminie.
7. Wnioskowane zmiany nie mogą skutkować zmianą, która może spowodować modyfikację punktacji przyznanej w ramach oceny Wniosku, ani naruszać kryteriów, które były podstawą oceny Projektu grantowego. Każda zmiana podlega weryfikacji i zatwierdzeniu przez KPG na podstawie odrębnego regulaminu. Grantobiorca jest zobowiązany do złożenia wniosku o zmianę wraz z uzasadnieniem zmiany.
8. Grantobiorca jest zobowiązany do utrzymania efektów Projektu Grantowego w okresie 3 lat od daty zatwierdzenia wniosku rozliczającego.
9. Grantobiorca jest zobowiązany do:
    a. utrzymania środków trwałych i usług nabytych w ramach Projektu grantowego,
    b. zapewnienia, że nie dojdzie do zmiany własności elementu infrastruktury,
    c. zapewnienie, że nie dojdzie do istotnej zmiany Projektu grantowego wpływającej na charakter Przedsięwzięcia grantowego, jego celów lub warunków wdrażania, która mogłaby doprowadzić do naruszenia jego pierwotnych celów,
    d. zapewnia środków finansowych na utrzymanie długoterminowych efektów Projektu grantowego.

§6 Zawarcie Umowy/Porozumienia

1. Wzór Umowy/Porozumienia o powierzenie grantu stanowi Załącznik nr 4 do Regulaminu.
2. Wraz z informacją o przyznaniu Grantu, Partner wzywa Wnioskodawcę grantu za pośrednictwem LSI, do dostarczenia dokumentów niezbędnych do zawarcia Umowy/Porozumienia o powierzenie grantu, wymienionych w Załączniku nr 5 do Regulaminu.

3. Umowa/Porozumienie o powierzenie grantu zostaje zawarta w formie elektronicznej.
4. Wnioskodawca grantu dostarcza Partnerowi dokumenty niezbędne do zawarcia Umowy/Porozumienia o powierzenie grantu w terminie 14 dni kalendarzowych 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, OOW może odmówić zawarcia Umowy/Porozumienia.
5. W razie zaistnienia okoliczności, o której mowa w ust. 4 powyżej, wybrany do wsparcia zostaje Projekt, które uzyskał następną w kolejności najwyższą liczbę punktów w ramach oceny kryteriów merytorycznych, o ile pozostająca kwota środków przeznaczonych na wsparcie Projektów w naborze pozwala pokryć całość wnioskowanej przez tego Wnioskodawcę kwoty wsparcia.
6. Postanowienia ust. 5 powyżej stosuje się również w sytuacji, gdy po zawarciu Umowy/Porozumienia Wnioskodawca odstępuje od jego realizacji.

§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: https://www.gov.pl/web/cppc/inwestycja-c-311konkurs-grantowy-cyberbezpieczny-rzad
3. Ewentualne pytania dotyczące Konkursu Grantowego Wnioskodawcy grantu mogą zgłaszać na **adres e-mail: cyberbezpiecznyrzad@cppc.pl oraz na infolinię obsługiwaną przez Partnera pod nr: +48 22 182 22 94.** Odpowiedzi polegające na wyjaśnieniu procedur będą dodatkowo zamieszczane w pytaniach i odpowiedziach.
4. W sprawach nieuregulowanych niniejszym Regulaminem mają zastosowanie obowiązujące przepisy prawa.
5. W przypadku zmiany Regulaminu, OOW zamieszcza na stronie internetowej Przedsięwzięcia informację o jego zmianie i terminie od kiedy zmiana obowiązuje.
6. OOW 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 wsparcie w formie grantu (Formularz Aplikacyjny);
2. Lista podmiotów uprawnionych do uczestniczenia w naborze;
3. Kryteria wyboru Projektów grantowych;
4. Wzór Umowy/Porozumienia o powierzenie grantu;
5. Lista dokumentów niezbędnych do podpisania Umowy/Porozumienia;
6. Klauzula informacyjna;
7. Opis wskaźników Przedsięwzięcia pod nazwą *„Cyberbezpieczny Rząd”*.