Regulamin Konkursu Grantowego pn.

“Cyberbezpieczne Wodociągi”

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

“Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi”.

Krajowy Plan Odbudowy i Zwiększania Odporności finansowany 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 niemających 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 (utrzymane przez okres 3 lat od zakończenia Projektu grantowego);
3. **Grant** – środki finansowe w formie pomocy de minimis, które Partner przekaże Grantobiorcy na podstawie Umowy o powierzenie grantu na realizację zadań służących osiągnięciu celu Projektu grantowego.
4. **Grantobiorca** – podmiot prowadzący działalność w zakresie zbiorowego zaopatrzenia w wodę objęty krajowym system cyberbezpieczeństwa, wykorzystujący technologie operacyjne w przemysłowych systemach sterowania, będący:

1) przedsiębiorstwem wodociągowo-kanalizacyjnym, które jest operatorem usług kluczowych w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222) (dalej: ustawa KSC) lub
2) spółką prawa handlowego wykonującą zadania o charakterze użyteczności publicznej w rozumieniu przepisów ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), lub
3) jednostką sektora finansów publicznych w rozumieniu art. 9 pkt 2–4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756

i 1907 oraz z 2025 r. poz. 39).

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; tj. Inwestycję C3.1.1 pn. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo.
7. **Pomoc de minimis** - pomoc udzielana na podstawie rozporządzenia Ministra Cyfryzacji z dnia 29 maja 2025 r. w sprawie udzielania pomocy de minimis na wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę objętych krajowym systemem cyberbezpieczeństwa, w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (Dz. U. poz. 729), zgodnie z przepisami rozporządzenia Komisji (UE) nr 2023/2831 z dnia 13 grudnia 2023 r. w sprawie stosowania art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej do pomocy de minimis (Dz. Urz. UE L 2023/2831 z 15.12.2023).
8. **Komisja Przyznająca Granty** – komisja oceniająca Wnioski o przyznanie grantu, zatwierdzająca listę rankingową Wniosków i wnioski o zmianę zakresu Projektu grantowego, według zasad określonych w niniejszym Regulaminie (dalej Komisja lub KPG);
9. **Konkurs Grantowy** – konkurs, o którym mowa w niniejszym Regulaminie, prowadzony przez OOW w celu wyłonienia Grantobiorców w naborze nr KPOD.05.10-CW.01-001/25 (dalej również Konkurs);
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 Konkursu oraz na stronie https://lsi.cppc.gov.pl/beneficjent;
11. **Partner** – Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy

(NASK-PIB);

12. **Projekt grantowy** - działania realizowane przez podmiot prowadzący działalność w zakresie zbiorowego zaopatrzenia w wodę prowadzone w ramach przedsięwzięcia, o którym mowa w art. 14la pkt 8 Ustawy, 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.

13. **Przedsięwzięcie** – Element Inwestycji C3.1.1. realizowany przez OOW, zmierzający do osiągnięcia założonego celu określonego wskaźnikami, z określonym początkiem i końcem realizacji. Przedsięwzięcie pn. “Cyberbezpieczne Wodociągi”, w ramach którego OOW udziela grantów Grantobiorcom na realizację zadań służących osiągnięciu celu tego Przedsięwzięcia - Wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę, objętych krajowym systemem cyberbezpieczeństwa, wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS), modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT.

14. **Regulamin Konkursu Grantowego lub Regulamin** – niniejszy Regulamin;

15. **Strona internetowa Konkursu** –https://www.gov.pl/web/cppc/start-naboru-cyberbezpieczne-wodociagi

16. **Umowa** lub **Umowa o powierzenie grantu** – umowa zawarta pomiędzy Grantobiorcą i OOW określająca w szczególności zakres Projektu grantowego, zadania Grantobiorcy objęte Grantem, kwotę Grantu, okres realizacji Umowy, warunki przekazania i rozliczenia Grantu- będąca jednocześnie umową o udzielenie pomocy de minimis, o której mowa w § 14 Rozporządzenie Ministra Cyfryzacji z dnia 29 maja 2025 r. w sprawie udzielania pomocy de minimis na wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę objętych krajowym systemem cyberbezpieczeństwa, w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (Dz. U. poz. 729).;

17. **Ustawa –** ustawa z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz.U. 2025 r. poz. 158)**;**

18. **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;**
19. **Wnioskodawca** – podmiot uprawniony do udziału w Konkursie Grantowym, który składa Wniosek.
20. **Wskaźniki przedsięwzięcia** – wskaźniki, których opis stanowi Załącznik nr 7 do Regulaminu Konkursu Grantowego;
21. **Wydatki faktycznie poniesione** – wydatki poniesione w znaczeniu kasowym, tj. jako rozchód środków pieniężnych z kasy lub rachunku płatniczego.

§ 2

Podstawy prawne

Konkurs Grantowy jest organizowany w oparciu o następujące akty prawne:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/241 z dnia 12 lutego2021 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) Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 ze zm.).
6) Rozporządzenie Ministra Cyfryzacji z dnia 29 maja 2025 r. w sprawie udzielania pomocy de minimis na wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę objętych krajowym systemem cyberbezpieczeństwa, w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (zwane także: Rozporządzeniem de minimis),

7) oraz w oparciu o:

   a) Decyzję z dnia 31.07.2025 r. nr KPOD.05.10-IW.06-008/25-00 o objęciu Przedsięwzięcia wsparciem pn. „Cyberbezpieczne Wodociągi”;

   b) Umowę o Partnerstwie z dnia 11 lipca 2025 r. zawartą przez OOW i Partnera.

§ 3

Informacje ogólne

1. Celem Przedsięwzięcia jest poprawa cyberbezpieczeństwa dla określonej grupy podmiotów krajowego systemu cyberbezpieczeństwa, o których mowa w § 4 ust. 1 poniżej, poprzez udzielenie im pomocy de minimis w formie grantów.
2. Konkurs realizowany jest przez OOW we współpracy z Partnerem.
3. Celem Konkursu jest wybór maksymalnie 552 Projektów grantowych, które 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 osiągnięty poprzez realizację Projektów grantowych.
4. Przedmiotem Konkursu jest wybór Grantobiorców, którzy będą realizować Projekty grantowe mające na celu osiągnięcie Wskaźników w zakresie i terminach określonych w Regulaminie.
5. Konkurs grantowy pn. „Cyberbezpieczne wodociągi” realizuje Przedsięwzięcie.
6. W ramach Konkursu Grant może otrzymać nie więcej niż 552 Wnioskodawców (wskaźnik Konkursu).
7. Dane osobowe Wnioskodawcy oraz osób wskazanych przez niego we Wniosku, w tym dane Projektu grantowego będą przetwarzane w ramach projektu w dwóch systemach: LSI – system do składania wniosków o grant, oraz SORG – system do rozliczeń grantów. Klauzula informacyjna zamieszczona jest na stronie internetowej CPPC pod adresem Przetwarzanie danych osobowych - Centrum Projektów Polska Cyfrowa - Portal Gov.pl, w zakładce “Beneficjenci, Partnerzy, Osoby uczestniczące i korzystające”, pod nazwą „Instrument na rzecz Odbudowy i Zwiększania Odporności (KPO) dla JW jako OOW”.

8. OOW przyzna Grantobiorcy Grant na zadania realizowane w ramach poniżej wskazanych obszarów:

1) **obszar organizacyjny**, który obejmuje wszelkie aspekty organizacyjne bezpieczeństwa systemów teleinformatycznych IT i OT, tj. audyt bezpieczeństwa, audyt zgodności z przepisami i normami, opracowanie, wdrożenie, utrzymanie i aktualizacja systemu zarządzania bezpieczeństwem informacji, systemu zarządzania bezpieczeństwem systemu teleinformatycznego IT/OT, systemu zarządzania ciągłością działania systemu teleinformatycznego IT/OT;

2) **obszar kompetencyjny**, który obejmuje wszelkie działania podnoszące świadomość, wiedzę i umiejętności na poziomie podstawowym, kierowniczym i specjalistycznym w zakresie cyberbezpieczeństwa, realizowane dla pracowników podmiotu, operatorów i administratorów systemów teleinformatycznych IT/OT, kadry kierowniczej IT/OT, kadry kierowniczej i zarządzającej podmiotu;

3) **obszar techniczny IT** (dotyczy obszaru funkcjonalnego IT), który obejmuje wszelkie komputerowe środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa komponentów środowiska teleinformatycznego IT, tj.: stacje robocze, serwery, dane biznesowe, oprogramowanie biznesowe, systemy pamięci masowej, urządzenia sieciowe i środowisko sieciowe IT;

4) **obszar techniczny OT** (dotyczy obszaru funkcjonalnego OT), który obejmuje wszelkie komputerowe środki techniczne i wybrane elektrotechniczne środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa w zakresie zbiorowego zaopatrzenia w wodę i zbiorowego odprowadzania ścieków, tj. komponentów środowiska teleinformatycznego OT/ICS/IIoT i środowiska IT obszaru przemysłowego OT, w tym: stacje robocze, serwery, dane systemów IT/OT/ICS/IIoT, systemy IT/OT/ICS/IIoT, oprogramowanie IT/OT/ICS/IIoT, urządzenia sieciowe i środowisko sieciowe IT/OT/ICS/IIoT oraz obejmuje rozwiązania zabezpieczenia systemów bezpieczeństwa wizyjnego, fizycznego i technicznego.

9. Niniejszy Regulamin określa zasady Konkursu i sposób wyboru Grantobiorców w ramach Konkursu Grantowego.

10. Konkurs Grantowy jest prowadzony na terenie całej Polski.
11. Grantobiorcy będą realizowali Projekty grantowe na podstawie Umowy zawartej pomiędzy Grantobiorcą a OOW.
12. Dopuszcza się kwalifikowalność wydatków poniesionych w Projekcie grantowym w okresie **od 01.01.2025 r**. do dnia zakończenia realizacji Projektu grantowego określonego w Umowie, jednakże nie dłużej niż do 30.06.2026 r.
13. Wydatki poniesione po terminie 30.06.2026 r. będą uznane za niekwalifikowalne.
14. Wniosek uznaje się za złożony, jeśli spełnia następujące warunki:
    1) został złożony w terminie, o którym mowa w § 6 ust. 1 pkt 2.
    2) został złożony zgodnie z zasadami określonymi w § 6 ust. 2.

§ 4

Podmioty uprawnione do udziału w Konkursie Grantowym

1. Do udziału w Konkursie Grantowym uprawnione są podmioty prowadzące działalność w zakresie zbiorowego zaopatrzenia w wodę objęte krajowym system cyberbezpieczeństwa, wykorzystujące technologie operacyjne w przemysłowych systemach sterowania, będące:
    1) przedsiębiorstwem wodociągowo-kanalizacyjnym, które jest operatorem usług kluczowych w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222) lub
    2) spółką prawa handlowego wykonującą zadania o charakterze użyteczności publicznej w rozumieniu przepisów ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), lub
    3) jednostką sektora finansów publicznych w rozumieniu art. 9 pkt 2–4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756 i 1907 oraz z 2025 r. poz. 39).
2. Podmiot, o którym mowa w ust. 1 musi spełniać warunki określone w kryterium formalnym - Kwalifikowalność Wnioskodawcy, opisane w Załączniku nr 2 do

Regulaminu - Kryteria wyboru Projektów grantowych.

§ 5

Zasady finansowania Projektów grantowych

1. Alokacja na Granty w Konkursie Grantowym pn. „Cyberbezpieczne Wodociągi” wynosi **313 000 000,00 PLN netto.**
2. W przypadku gdy założona kwota alokacji środków nie pozwoli na realizację zakładanego wskaźnika minimalnej liczby podmiotów objętych wsparciem, OOW dopuszcza możliwość zwiększenia alokacji Przedsięwzięcia.
3. Wysokość przyznanego Grantu dla Projektu grantowego wynosi **100% kosztów kwalifikowalnych**.
4. Minimalna wysokość grantu, o jaką może wnioskować jeden Wnioskodawca to wartość 130 000 PLN.
5. Maksymalna wysokość Grantu dla jednego Wnioskodawcy uzależniona jest od wysokości przyznanej mu pomocy de minimis, której całkowita kwota nie może przekroczyć 300 000 EUR w okresie trzech lat.
6. Kurs euro, wg którego Wnioskodawca powinien obliczyć maksymalny limit dla wnioskowanej wysokości kwoty Grantu wynosi 4,2661 zł. (źródło: Narodowy Bank Polski, Tabela nr 147/A/NBP/2025 z dnia wydania Decyzji nr KPOD.05.10-IW.06-0008/25-00 o objęciu wsparciem Przedsięwzięcia tj. 31 lipca 2025 roku). Limit, o którym mowa powyżej, ustalany jest wyłącznie na potrzeby przeprowadzenia oceny Wniosku. Ostateczna wysokość limitu możliwej do przyznania danemu Wnioskodawcy pomocy de minimis, ustalana będzie na zasadach opisanych w § 8 ust. 5.
7. Wskazane przez Wnioskodawcę kwoty weryfikowane będą na podstawie zaświadczeń albo oświadczeń i informacji o otrzymanej pomoc de minimis, stanowiących Załącznik nr 5 i 10 do Regulaminu.
8. Podmiot, który otrzymał pomoc de minimis (stanowiącą rekompensatę za realizację usług świadczonych w ogólnym interesie gospodarczym) w rozumieniu

rozporządzenia 2023/2832 w pełnej wysokości 750 000 EUR w ciągu 3 lat może wciąż uzyskać pomoc de minimis w rozumieniu rozporządzenia 2023/2831 w pełnej wysokości 300 000 EUR w ciągu 3 lat (obie pomoce de minimis można ze sobą łączyć).

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

1) Sprzęt informatyczny i urządzenia bezpieczeństwa IT/OT/ICS/IIoT:

Katalog kosztów kwalifikowalnych w zakresie sprzętu informatycznego i urządzeń bezpieczeństwa obejmuje sprzęt i urządzenia, których zastosowanie może przyczynić się do zabezpieczenia i zwiększenia odporności rozwiązań teleinformatycznych klasy IT w obszarze IT oraz rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT w obszarze OT.

Katalog obejmuje sprzęt i urządzenia, które, w zależności od typu i modelu, realizują funkcje tylko w wybranych środowiskach IT, OT, ICS, IIoT. Ich funkcje, przeznaczenie i zastosowanie są zdeterminowane przez i zależne od zastosowania do rozwiązań teleinformatycznych klasy IT w obszarze IT i/lub rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT w obszarze OT.

Katalog zawiera również sprzęt i urządzenia dedykowane tylko dla rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT w obszarze OT, które zostały oznaczone symbolem i kolejnym numerem – OT1 do OT3 oraz rozwiązania zapewniające ciągłość działania rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT w obszarze IT i OT oraz systemów bezpieczeństwa w obszarach IT i OT w przypadku braku zasilania, które zostały oznaczone symbolem i kolejnym numerem – Z1 do Z4.

Lp.	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 Streamer’a	S15
16	Macierz dyskowa	S16

Lp.	Nazwa produktu	Symbol produktu
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	System monitorujący pracę urządzeń sieciowych i serwerów	S28
29	Klucze sprzętowe U2F	S29
30	Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa	S30
31	Urządzenia do zabezpieczania dowodów cyfrowych	S31

Lp.	Nazwa produktu	Symbol produktu
32	Urządzenia HSM	S32
33	Urządzenia do zarządzania PKI	S33
34	Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise	S34
35	Stacja robocza fizyczna lub wirtualna z rolą stacji przesiadkowej	S35
36	LoRaWan Gateway	OT1
37	Bramy jednokierunkowe (Unidirectional Gateway / Data Diode)	OT2
38	Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych)	OT3
39	Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa	Z1
40	Akumulatory do urządzeń typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa	Z2
41	Agregat prądotwórczy	Z3
42	Mobilny agregat prądotwórczy	Z4

2) Oprogramowanie bezpieczeństwa IT/OT/ICS/IIoT:

Katalog kosztów kwalifikowalnych w zakresie oprogramowania bezpieczeństwa obejmuje oprogramowanie, którego zastosowanie może przyczynić się do zabezpieczenia i zwiększenia odporności rozwiązań teleinformatycznych klasy IT w obszarze IT oraz rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT w obszarze OT.

Katalog obejmuje oprogramowanie, które, w zależności od typu i modelu, realizuje funkcje tylko w wybranych środowiskach IT, OT, ICS, IIoT. Ich funkcje, przeznaczenie i

zastosowanie są zdeterminowane przez i zależne od zastosowania do rozwiązań teleinformatycznych klasy IT w obszarze IT i/lub rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT w obszarze OT.

Lp.	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 / licencje IPS (Intrusion Prevention System)	O05
6	Oprogramowanie / licencje IPS (Intrusion Prevention System) dedykowany sieciom OT	O06
7	Oprogramowanie / licencje IDS (Intrusion Detection System)	O07
8	Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT	O08
9	Oprogramowanie / licencje VPN (Virtual Private Network)	O09
10	Oprogramowanie / licencje NAC (Network Access Control)	O10
11	Oprogramowanie typu MDM (Mobile Device Management)	O11
12	Oprogramowanie typu EDR (Endpoint Detection and Response)	O12
13	Oprogramowanie typu XDR (Extended Detection and Response)	O13

Lp.	Nazwa produktu	Symbol produktu
14	Oprogramowanie typu NDR (Network Detection & Response)	O14
15	Oprogramowanie typu ITDR (Identity Threat Detection and Response)	O15
16	Oprogramowanie do wykonywania kopii zapasowych (w tym deduplikacji)	O16
17	Oprogramowanie antyspamowe	O17
18	Oprogramowanie WAF (Web Application Firewall)	O18
19	Oprogramowanie SIEM (Security Information and Event Management)	O19
20	Oprogramowanie SOAR (Security Orchestration, Automation and Response)	O20
21	Oprogramowanie SASE VPN	O21
22	Oprogramowanie typu Network Security Policy Management & Orchestration	O22
23	Oprogramowanie typu HoneyPot	O23
24	Oprogramowanie typu Menadżer logów	O24
25	Oprogramowanie do zarządzania podatnościami	O25
26	Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP – Data Leak Prevention)	O26
27	Oprogramowanie do zarządzania uprzywilejowanego	O27

Lp.	Nazwa produktu	Symbol produktu
	dostępu (PAM- Privileged Access Management/ PIM - Privileged Identity Management)	
28	Oprogramowanie typu BAS (Breach and attack simulation)	O28
29	Oprogramowanie Web Secure Gateway	O29
30	Oprogramowanie Email Secure Gateway	O30
31	Oprogramowanie do zarządzania tożsamością i dostępem	O31
32	Oprogramowanie centralnego menadżera haseł	O32
33	Oprogramowanie do monitorowania infrastruktury informatycznej	O33
34	Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych	O34
35	Oprogramowanie do badania podatności systemów informatycznych	O35
36	Oprogramowanie do badania podatności serwisów WWW	O36
37	Oprogramowanie do badania podatności w kodzie aplikacji	O37
38	Oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików	O38
39	Oprogramowanie do analizy powłamaniowej	O39
40	Oprogramowanie do ochrony przed ransomware	O40

Lp.	Nazwa produktu	Symbol produktu
41	Oprogramowanie typu ITSM (Information Technology Service Management)	O41
42	Oprogramowanie typu SoftHSM	O42
43	Oprogramowanie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie)	O43
44	Certyfikaty SSL serwisów internetowych	O44
45	Oprogramowanie ochrony AntyDDoS	O45
46	System wirtualizacyjny dedykowany do systemów, na których zostanie zainstalowanych produkt z zakresu cyberbezpieczeństwa	O46
47	System operacyjny i/lub licencje dostępowe (również rozbudowa licencji do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa	O47
48	Systemy platform kontenerowych na których zostaną zainstalowane systemu z zakresu cyberbezpieczeństwa	O48
49	Oprogramowanie klasy RADIUS	O49
50	Infrastruktura PKI wraz z niezbędnymi elementami	O50
51	System klasy GRC	O51

3) Usługi bezpieczeństwa IT/OT/ICS/IIoT:

Katalog kosztów kwalifikowalnych w zakresie usług bezpieczeństwa obejmuje usługi, których zastosowanie może przyczynić się do zabezpieczenia i zwiększenia odporności

rozwiązań teleinformatycznych klasy IT w obszarze IT oraz rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT w obszarze OT oraz usługi związane z realizacją lub wdrożeniem rozwiązań obszarowych bezpieczeństwa, wskazanych w ramach obszarów organizacyjnego, kompetencyjnego oraz technicznego IT i technicznego OT.

Katalog obejmuje usługi, które, w zależności od kontekstu, celu i zakresu, mogą być realizowane tylko w wybranych środowiskach IT, OT, ICS, IIoT. Ich kontekst, cel, zakres i zastosowanie są zdeterminowane przez i zależne od zastosowania do rozwiązań obszarowych bezpieczeństwa, wskazanych w ramach obszarów organizacyjnego, kompetencyjnego oraz technicznego IT i technicznego OT.

Lp.	**Nazwa usługi**	**Symbol usługi**
1	Usługa poczty elektronicznej w chmurze obliczeniowej typu IaaS, SaaS, PaaS z rozwiązaniami bezpieczeństwa	U01
2	Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT	U02
3	Testy bezpieczeństwa serwisów internetowych IT/OT/ICS	U03
4	Testy bezpieczeństwa aplikacji IT/OT/ICS/IIoT	U04
5	Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS w zakresie sandbox do badania bezpieczeństwa aplikacji oraz plików IT/OT/ICS	U05
6	Usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego IT/OT/ICS	U06
7	Usługa w chmurze obliczeniowej SASE VPN IT/OT/ICS	U07
8	Usługa w chmurze obliczeniowej MDM (Mobile Device Management) IT/OT/ICS	U08
9	Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu	U09

Lp.	Nazwa usługi	Symbol usługi
	bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IIoT	
10	Utrzymanie i eksploatacja urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IIoT	U10
11	Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT	U11
12	Usługa SOC (Security Operation Center) IT/OT/ICS/IIoT	U12
13	Usługa CTI (Cyber Threat Intelligence) IT/OT/ICS/IIoT	U13
14	Usługi typu security awareness do symulowanych ataków socjotechnicznych IT/OT/ICS	U14
15	Usługa ochrony AntyDDoS IT/OT/ICS/IIoT	U15
16	Usługa kopii zapasowych w chmurze obliczeniowej IT/OT/ICS	U16
17	Usługa redundancji w chmurze obliczeniowej IT/OT/ICS	U17
18	Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT/ICS/IoT	U18
19	Nadzór nad realizacją/wdrożeniem zaprojektowanego rozwiązania z zakresu bezpieczeństwa IT/OT/ICS/IoT	U19
20	Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	U20

Lp.	Nazwa usługi	Symbol usługi
21	Utrzymanie, zarządzanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	U21
22	Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI	U22
23	Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Ciągłością Działania STI (SZCD)	U23
24	Utrzymanie, zarządzanie i doskonalenie Systemu Zarządzania Ciągłością Działania STI (SZCD)	U24
25	Audyt SZBI, audyt SZCD, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów, audyt (re)certyfikacji SZBI, SZCD na zgodność z normami IT/OT/ICS	U25
26	Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników IT/OT/ICS	U26
27	Szkolenia z zakresu cyberbezpieczeństwa – szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji IT/OT/ICS	U27
28	Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS	U28
29	Szkolenia z zakresu cyberbezpieczeństwa - szkolenia	U29

Lp.	Nazwa usługi	Symbol usługi
	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 IT/OT/ICS	
30	Szkolenia symulacyjne z zakresu cyberbezpieczeństwa, ciągłości działania, zarządzania kryzysowego	U30
31	Certyfikacja z zakresu cyberbezpieczeństwa: wyrobów (urządzeń i oprogramowania), usług i procesów, certyfikacja kompetencji (osób) IT/OT/ICS	U31
32	Szkolenia przygotowujące do certyfikacji z zakresu cyberbezpieczeństwa IT/OT/ICS	U32
33	Usługa inwentaryzacji aktywów teleinformatycznych IT/OT/ICS/IIoT	U33
34	Doradztwo w zakresie opracowania warunków umów kontraktowych na wdrożenie i utrzymanie infrastruktury w zakresie cyberbezpieczeństwa, obejmujących m.in. łańcuch dostaw, infrastrukturę monitorowania i zarządzania, usługi zdalne, itp. IT/OT/ICS/IIoT	U34
35	Przyłącze elektryczne do agregatu prądotwórczego (projekt, wykonanie)	U35
36	Usługa typu MIDS (Managed Intrusion Detection System) IT/OT/ICS	U36
37	Audyt cyberbezpieczeństwa sieci IT/OT/ICS/IIoT	U37

Lp.	Nazwa usługi	Symbol usługi
38	Usługi reagowania na incydenty w środowisku IT/OT/ICS	U38
39	Usługi konfiguracji i hardeningu systemów/urządzeń IT/OT/ICS/IIoT	U39
40	Usługa Private APN	U40
41	Usługa segmentacji sieci IT/OT/ICS/IIoT	U41
42	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	U42
43	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	U43

11. Kwalifikowalne będą tylko koszty poniesione w okresie realizacji Projektu grantowego, z zastrzeżeniem ust. 12.
12. Wydatki faktycznie poniesione w okresie kwalifikowalności na ubezpieczenia i gwarancje zostaną uznane za koszty kwalifikowalne, pod warunkiem ich zsumowania z wydatkami na zakup sprzętu i urządzeń bezpieczeństwa poniesionymi w ramach Projektu grantowego i ze środków Grantu. Wydatki te mogą dotyczyć wyłącznie

ubezpieczeń i gwarancji świadczonych maksymalnie do końca okresu, o którym mowa w §1 ust. 2 Regulaminu.

13. Kwalifikowalne będą również koszty poniesione w okresie realizacji Projektu grantowego na informację i promocję Projektu grantowego – symbol tego kosztu we Wniosku jest oznaczony jako IP1. Limit na wydatki na informację i promocję projektu nie może przekraczać 5% całkowitej kwoty przyznanego grantu, ani kwoty 10 000,00 PLN.
14. 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 Projekt grantowy (m.in. inżynier kontraktu, ekspert z dziedziny cyberbezpieczeństwa).
15. 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, a środki poniesione na ich cel podlegać będą zwrotowi wraz z odsetkami.
16. Łączny limit wydatków w ramach rozwiązań zapewniających ciągłość działania systemów bezpieczeństwa w obszarach IT i OT w przypadku braku zasilania, które zostały oznaczone symbolami produktu Z1 do Z4 w tabeli w ust. 10 pkt 1 (Sprzęt informatyczny i urządzenia bezpieczeństwa IT/OT/ICS/IIoT) oraz symbolem produktu U35 w tabeli w ust. 10 pkt 3 (Usługi bezpieczeństwa IT/OT/ICS/IIoT), wynosi maksymalnie 20% wartości otrzymanego Grantu.
17. Do **wydatków niekwalifikowanych** w ramach Grantu zalicza się w szczególności wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa, w szczególności:

1) komputery stacjonarne (z wyłączeniem stacji roboczych fizycznych lub wirtualnych, pełniących rolę stacji przesiadkowej, stanowiących koszty kwalifikowalne – poz. S35) i komputery przenośne;
2) niezarządzalne urządzenia sieciowe;
3) wymiana i/lub doposażenie stacji roboczych z peryferiami;
4) akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki);
5) urządzenia mobilne (smartfony, tablety);
6) wymiana i/lub doposażenie serwerów dedykowanych do systemów dziedzinowych, niezwiązane z wdrożeniem rozwiązań bezpieczeństwa;
7) materiały eksploatacyjne;
8) oprogramowanie biurowe, oprogramowanie do elektronicznego zarządzania dokumentacją i oprogramowanie systemów operacyjnych, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;
9) szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;
10) usługi dostępu do Internetu, abonamenty telefoniczne;
11) budowa infrastruktury sieci LAN/WAN/Radiowej/Światłowodowej w obszarach IT i OT;
12) rozwiązania dziedzinowe obszarów OT/ICS/IIoT, np. SCADA, HMI, itp.;
13) infrastruktura rozwiązań dziedzinowych obszarów OT/ICS/IIoT, np. SCADA, HMI, itp.;
14) systemy telemetryczne i komponenty systemów telemetrycznych;
15) rozwiązania bezpieczeństwa wizyjnego, fizycznego i technicznego;
16) rozwiązania w zakresie ochrony informacji niejawnych.

§ 6

Zasady i sposób naboru Wniosków

1. **Nabór Wniosków:**

    1) Wnioski zostaną wybrane w Konkursie w otwartym naborze Wniosków, z zachowaniem zasady bezstronności i przejrzystości.

    2) Nabór Wniosków trwać będzie od 01.09.2025 r. do 02.10.2025 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 Konkursu będą publikowane na Stronie internetowej Konkursu wraz ze wskazaniem terminów składania Wniosków.

2. **Sposób składania Wniosków**

    1) Wzór Wniosku jest dostępny na Stronie internetowej Konkursu oraz stanowi Załącznik nr 1 do Regulaminu. Wnioskodawca zobowiązany jest do zapoznania się i stosowania instrukcji, dostępnej pod adresem Instrukcje użytkownika systemu LSI - Centrum Projektów Polska Cyfrowa - Portal Gov.pl

    2) Wniosek należy wypełnić za pomocą systemu LSI, zgodnie z Instrukcją, która stanowi Załącznik nr 13 do Regulaminu.

    3) Złożenie Wniosku oznacza, że Wnioskodawca zapoznał się z Regulaminem Konkursu Grantowego wraz z Załącznikami do Regulaminu i akceptuje ich warunki.

    4) Wraz z Wnioskiem Wnioskodawca składa Załączniki Nr 4, 5, 10, 11 i 12 do Regulaminu.

    5) Wnioskodawca na każdym etapie ma możliwość wycofania Wniosku przesyłając za pośrednictwem LSI pismo z informacją o wycofaniu z Konkursu Grantowego, podpisane elektronicznie zgodnie z reprezentacją Wnioskodawcy.

    6) Wnioskodawca uprawniony jest do złożenia jednego Wniosku w Konkursie Grantowym. W przypadku złożenia większej liczby Wniosków, oceniany będzie ten złożony jako pierwszy, a pozostałe wnioski zostaną pozostawione bez

rozpoznania.

7) Wniosek powinien być złożony przez Wnioskodawcę i opatrzony kwalifikowalnym podpisem elektronicznym przez osobę/osoby upoważnioną/e do reprezentacji Wnioskodawcy. Do Wniosku należy dołączyć dokumenty potwierdzające umocowanie danej osoby/osób do reprezentowania Wnioskodawcy.

8) Wnioskodawca 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 Wniosków do Konkursu Grantowego.

§ 7

Zasady oceny Wniosków

1. O przyznaniu Grantu w naborze i w naborze uzupełniającym decyduje pozytywny wynik oceny formalnej i merytorycznej Wniosku oraz pozycja na liście rankingowej.
2. Ocena Wniosku będzie dokonywana przez Komisję Przyznającą Granty, na podstawie ocen cząstkowych, przyznawanych przez ekspertów na etapie oceny formalnej i merytorycznej w systemie LSI. KPG będzie działała na podstawie odrębnego regulaminu prac Komisji.
3. Ocena Wniosków trwa do 60 dni kalendarzowych liczonych od dnia zakończenia Konkursu. W przypadku gdy w ramach Konkursu zostanie złożonych więcej niż 450 Wniosków, czas na ocenę Wniosków może zostać wydłużony.
4. Wnioski zostaną poddane ocenie formalnej i merytorycznej w oparciu o kryteria wyboru Projektów grantowych, określone w Załączniku nr 2 do Regulaminu.
5. W zakresie oceny formalnej zostanie zweryfikowane, czy Wnioskodawca 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 oceny formalnej i był przekazany do oceny merytorycznej, musi spełnić wszystkie kryteria oceny formalnej.
8. W przypadku stwierdzenia we Wniosku uchybień lub braków formalnych, o których mowa w §10 ust. 6 Rozporządzenia de minimis, 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, o którym mowa w ust. 8 zostanie przekazane Wnioskodawcy za pomocą LSI.
10. Wnioskodawca grantu będzie miał 7 dni kalendarzowych od dnia wysłania wezwania, o którym mowa w ust. 8, 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. Jeżeli Wniosek nie zostanie uzupełniony w terminie, o którym mowa w ust. 10, pozostawia się go bez rozpoznania, a Wnioskodawca otrzymuje w LSI informację o negatywnym wyniku oceny formalnej.
12. W zakresie oceny merytorycznej zostanie zweryfikowane czy Wniosek spełnia zdefiniowane kryteria oceny merytorycznej.
13. Kryteria merytoryczne nr 1, 2, 3 i 5 wskazane w Załączniku nr 2 do Regulaminu (Kryteria wyboru Projektów grantowych dla Przedsięwzięcia pod nazwą „Cyberbezpieczne Wodociągi”) mają charakter zero - jedynkowy (zasada: nie spełnia - 0; spełnia - 1). Wniosek musi spełniać każde z tych kryteriów.
14. 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, z zastrzeżeniem ust. 15.
15. W zakresie kryterium merytorycznego nr 4, Wnioskodawca musi otrzymać minimum 6 punktów, aby kryterium uznać za spełnione.

16. W przypadku otrzymania przez kilku Wnioskodawców takiej samej liczby punktów w ramach przeprowadzonej oceny merytorycznej, o kolejności Projektu grantowego na liście rankingowej decyduje kolejność złożenia Wniosku przez Wnioskodawcę.
17. Ocena merytoryczna Wniosku w części dotyczącej kryterium merytorycznego nr 4. *Ocena planowanego zakresu postępu Projektu grantowego* obejmuje analizę zbioru produktów, działań i usług bezpieczeństwa, uporządkowanych w ramach określonych *Rozwiązań obszarowych bezpieczeństwa*. Ocenie podlega zarówno obecny, jak i docelowy ich zakres i poziom.
18. *Rozwiązania obszarowe bezpieczeństwa* w ramach prowadzonych Projektów grantowych powinny dotyczyć wskazanych w poniższej tabeli obszarów:

Lp.	**Obszary**	**Rozwiązanie obszarowe bezpieczeństwa**	**Premia**
1	Organizacyjny	1.1 Systemowe zarządzanie bezpieczeństwem i ciągłością działania IT/OT	-
2	Kompetencyjny	2.1 Szkolenia z zakresu cyberbezpieczeństwa	+50%
3	Techniczny IT	3.1 Bezpieczeństwo systemów informatycznych	-
4	Techniczny IT	3.2 Bezpieczeństwo www (stron i/lub platform internetowych)	-
5	Techniczny IT	3.3 Bezpieczeństwo stacji roboczych	-
6	Techniczny IT	3.4 Rozwiązanie bezpieczeństwa sieci	+50%
7	Techniczny IT	3.5 Rozwiązania bezpieczeństwa styku sieci Internet z usługami wewnętrznymi	+50%

Lp.	Obszary	Rozwiązanie obszarowe bezpieczeństwa	Premia
8	Techniczny IT	3.6 Zwiększenie niezawodności i wydajności	-
9	Techniczny IT	3.7 Rozwiązania sieciowe WAN/LAN/Wi-Fi	-
10	Techniczny IT	3.8 Rozwiązania wirtualizacyjne	-
11	Techniczny IT	3.9 Rozwiązania kopii zapasowych	-
12	Techniczny IT	3.10 Redundancja (HA)	-
13	Techniczny IT	3.11 Rozwiązania zarządzania operacyjnego	-
14	Techniczny IT	3.12 Bezpieczeństwo komunikacji	-
15	Techniczny IT	3.13 Monitorowanie bezpieczeństwa	+50%
16	Techniczny IT	3.14 Reagowanie w zakresie bezpieczeństwa	-
17	Techniczny IT	3.15 Zarządzanie uprawnieniami użytkowników	+50%
18	Techniczny IT	3.16 Zabezpieczanie dowodów cyfrowych IT, OT/ICS/IIoT	-
19	Techniczny	4.1 Bezpieczeństwo systemów sterowania	+50%

Lp.	Obszary	Rozwiązanie obszarowe bezpieczeństwa	Premia
	OT	przemysłowego (OT/ICS/IIoT)	
20	Techniczny OT	4.2 Bezpieczeństwo stacji roboczych OT/ICS	+50%
21	Techniczny OT	4.3 Rozwiązania bezpieczeństwa sieci OT/ICS/IIoT	+50%
22	Techniczny OT	4.4 Rozwiązania sieciowe WAN/LAN/Wi-Fi OT/ICS/IIoT	+50%
23	Techniczny OT	4.5 Rozwiązania bezpieczeństwa styku sieci Internet z siecią OT/ICS/IIoT	+50%
24	Techniczny OT	4.6 Rozwiązania bezpieczeństwa styku sieci wewnętrznej IT z siecią OT/ICS/IIoT	+50%
25	Techniczny OT	4.7 Rozwiązania kopii zapasowych konfiguracji i danych systemów OT/ICS/IIoT	+50%
26	Techniczny OT	4.8 Redundancja (HA) OT/ICS/IIoT	+50%
27	Techniczny OT	4.9 Rozwiązania zarządzania operacyjnego infrastrukturą OT/ICS/IIoT	+50%
28	Techniczny OT	4.10 Monitorowanie bezpieczeństwa OT/ICS/IIoT	+50%
29	Techniczny OT	4.11 Reagowanie w zakresie bezpieczeństwa OT/ICS/IIoT	+50%
30	Techniczny OT	4.12 Zabezpieczenie systemów bezpieczeństwa wizyjnego, fizycznego i technicznego SUW	+50%

Lp.	Obszary	Rozwiązanie obszarowe bezpieczeństwa	Premia
		(Stacji Uzdatniania Wody), punktów ujęć wody, przepompowni i oczyszczalni ścieków działających w sieci	
31	Techniczny OT	4.13 Wsparcie ciągłości działania rozwiązań teleinformatycznych klasy IT, OT, ICS, IIoT obszaru IT i OT	+50%

19. Przyrost odporności na cyberzagrożenia jest obliczany jako różnica wartości sumy punktów docelowego i obecnego poziomu wszystkich *Rozwiązań obszarowych bezpieczeństwa*.
20. W części merytorycznej do Wniosku, przygotowanym na formularzu stanowiącym Załącznik nr 4, Wnioskodawca dla każdego stosowanego obecnie i docelowego *Rozwiązania obszarowego bezpieczeństwa* dokonuje samooceny zakresu i poziomu jego wdrożenia.
21. Wskazanie w formularzu stanowiącym Załącznik nr 4 obecnie wdrożonych i docelowych, planowanych do wdrożenia produktów, działań i usług bezpieczeństwa, dla każdego z *Rozwiązań obszarowych bezpieczeństwa*, jest realizowane poprzez:
    1) zaznaczenie wyboru z predefiniowanej listy pozycji najczęściej stosowanych w realizacji produktów, działań lub usług bezpieczeństwa;
    2) dodanie, gdy niezbędne, innych pozycji ze zbioru pozycji kosztów kwalifikowalnych;
    3) dodanie, gdy niezbędne, innych pozycji spoza zbioru pozycji kosztów kwalifikowalnych, przy czym pozycje te muszą należeć do rozwiązań zdefiniowanych dla obszarów organizacji, kompetencji i technologii (IT lub OT).
22. Każde *Rozwiązanie obszarowe bezpieczeństwa* wskazane w formularzu stanowiącym Załącznik nr 4 oceniane jest, dla stanu obecnego i docelowego, w skali punktowej z przedziału (0-3). Poszczególne wartości reprezentują zakres i poziom jego funkcjonowania i należy je rozumieć odpowiednio jako:

1) 0 – brak rozwiązania obszarowego bezpieczeństwa: niezakupione żadne produkty, usługi lub rozwiązania bezpieczeństwa lub zakupione pojedyncze produkty (oprogramowanie lub sprzęt) ale niewdrożone;
2) 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;
3) 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;
4) 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.

23. Procedura samooceny do wskazania w formularzu stanowiącym Załącznik nr 4 obecnych i docelowych, planowanych do wdrożenia *Rozwiązań obszarowych bezpieczeństwa*, polega na przeprowadzeniu dla każdego z nich następujących kroków:
    1) wskazanie dla predefiniowanej listy produktów, działań i usług tych, które są **obecnie** wdrożone i stosowane, poprzez wybór z listy opcji pozycji TAK lub NIE,

2) wskazanie dla predefiniowanej listy produktów, działań i usług tych, które są **docelowe** (planowane do realizacji) i stanowić będą docelowe elementy składowe, poprzez wybór z listy opcji pozycji TAK lub NIE,

3) wskazanie dla predefiniowanej listy produktów, działań i usług tych, których realizacja będzie objęta finansowaniem z Grantu, poprzez wybór z listy opcji pozycji TAK lub NIE,

4) w przypadku stosowania lub planowania produktów, działań i usług innych niż predefiniowane, wprowadzenie dodatkowych pozycji z listy lub spoza listy kosztów kwalifikowanych,

5) scharakteryzowanie i opisanie stanu obecnego i docelowego danego *Rozwiązania obszarowego bezpieczeństwa* (krótko, ok. 200-250 znaków),

6) ocenienie zakresu i poziomu danego *Rozwiązania obszarowego bezpieczeństwa* dla stanu obecnego i stanu docelowego w skali punktowej z przedziału (0-3), zgodnie z zasadami z pkt 22, poprzez wybór z listy dostępnych opcji (0,1,2,3).

24. Podczas oceny premiowane są *Rozwiązania obszarowe bezpieczeństwa* uznane za podnoszące w największym stopniu odporność i mitygujące w największym stopniu aktualnie cyberzagrożenia. Spośród 31 *Rozwiązań obszarowych bezpieczeństwa* 18 będzie dodatkowo punktowane premią 50% w ramach oceny kryterium merytorycznego nr 4.

25. W przypadku stwierdzenia błędów lub braków we Wniosku uniemożliwiających przeprowadzenie oceny merytorycznej, w tym uwzględnienia w nim wydatków niezgodnych z zakresem kosztów kwalifikowalnych KPG skieruje za pośrednictwem LSI do Wnioskodawcy grantu wezwanie, w zakresie poprawy lub uzupełnienia Wniosku o przyznanie grantu. Wnioskodawca grantu będzie miał 7 dni kalendarzowych od dnia wysłania wezwania na poprawę lub uzupełnienie Wniosku zgodnie z wezwaniem.

26. W przypadku braku poprawy lub uzupełnienia Wniosku o przyznanie grantu, zgodnie z treścią wezwania, o którym mowa w ust. 25, lub ich zakwestionowaniu przez Wnioskodawcę, KPG przekazuje Wnioskodawcy ponowne wezwanie do uzupełnienia lub poprawy Wniosku o przyznanie grantu w terminie 4 dni kalendarzowych od dnia

jego wysłania wraz z adnotacją, iż niezastosowanie się do wezwania skutkuje obniżeniem wartości kwoty Grantu o koszty niekwalifikowalne wskazane w wezwaniu.

27. Jeżeli Wnioskodawca nie poprawi lub nie uzupełni Wniosku o przyznanie grantu w terminie lub zakresie wskazanym w wezwaniu, o którym mowa w ust. 25 lub 26, KPG ocenia złożony pierwotnie Wniosek o przyznanie grantu.
28. W przypadku, gdy we Wniosku o przyznanie grantu został wskazany koszt niekwalifikujący się do sfinansowania, następuje usunięcie całej pozycji kosztowej.
29. W przypadku decyzji KPG w zakresie kwalifikowalności wydatków i obniżenia wartości kwoty grantu o koszty niekwalifikowalne, Wnioskodawcy nie przysługuje możliwość odwołania lub inny środek zaskarżenia od decyzji KPG.
30. Jeżeli w wyniku usunięcia wydatków niezgodnych z zakresem kosztów kwalifikowalnych, o czym mowa w ust. 29, nastąpi obniżenie kwoty grantu poniżej wartości, o której mowa w §5 ust. 4, wówczas Wniosek przestaje spełniać kryteria formalne i jest oceniany negatywnie.
31. Jeżeli koniec terminu do poprawy lub uzupełnienia wniosku przypada na dzień uznany ustawowo za wolny od pracy lub na sobotę, termin upływa następnego dnia, który nie jest dniem wolnym od pracy ani sobotą.
32. Fakt, że dany Projekt grantowy został zakwalifikowany do otrzymania grantu nie oznacza, że wszystkie koszty poniesione podczas jego 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 na etapie realizacji zostały uznane za niekwalifikowalne, pomimo uznania kosztu, na etapie oceny Wniosku, za kwalifikowalny. Grantobiorca ponosi także odpowiedzialność za skutki niewłaściwego zarządzania i dokumentowania 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.
33. Prawdziwość oświadczeń i danych zawartych we Wniosku może być weryfikowana w trakcie oceny formalnej i merytorycznej, jak również przed i po zawarciu Umowy.

34. Wnioskodawca ma prawo dostępu do dokumentów związanych z oceną złożonego przez siebie Wniosku, z zastrzeżeniem, że dane osobowe członków KPG i ekspertów dokonujących oceny nie podlegają ujawnieniu.
35. Projekt grantowy może być oceniony pozytywnie, jeżeli jednocześnie:
    1) spełnił zero-jedynkowe (spełnia/nie spełnia) kryteria wyboru Projektów grantowych i uzyskał wymaganą liczbę punktów na etapie oceny merytorycznej;
    2) Wnioskodawca grantu nie został wykluczony z możliwości otrzymania Grantu na podstawie przepisów odrębnych.
36. Po przeprowadzeniu oceny Wniosków Komisja Przyznająca Granty zatwierdzi listę rankingową. Lista rankingowa będzie zawierać informacje o wszystkich złożonych w naborze Wnioskach.
37. Wnioski na liście rankingowej będą ułożone w kolejności od najwyższej do najniższej sumy otrzymanych punktów z oceny merytorycznej, a w przypadku wskazanym w §7 ust. 16, także z uwzględnieniem kolejności złożenia Wniosku.
38. OOW publikuje listę rankingową, na stronie internetowej Konkursu. Granty otrzymają Wnioski z najwyższą uzyskaną oceną punktową, z zastrzeżeniem, że Granty zostaną przyznane nie więcej niż 552 Wnioskodawcom, zgodnie z limitem wynikającym ze wskaźnika Konkursu, o którym mowa w § 3 ust. 6 oraz do wysokości dostępnej alokacji.
39. OOW przewiduje możliwość aktualizacji listy rankingowej, w uzasadnionych przypadkach.
40. Informacja o wyniku oceny zostanie wysłana przez LSI do Wnioskodawców. Wynik oceny Wniosku jest ostateczny i nie podlega procedurze odwoławczej. Wnioskodawca nie ma możliwości złożenia odwołania, zażalenia ani innych środków prawnych w celu zakwestionowania wyników oceny.
41. Informacja o wyniku oceny zawiera uzasadnienie oceny, w tym, w zależności od okoliczności, informację o wystąpieniu wad formalnych, niespełnieniu poszczególnych kryteriów.

§ 8

Zawarcie Umowy

1. Wzór Umowy o powierzenie grantu stanowi Załącznik nr 3 do Regulaminu.
2. Wraz z informacją o przyznaniu Grantu, Partner wzywa Wnioskodawcę grantu za pośrednictwem LSI, do dostarczenia dokumentów niezbędnych do zawarcia Umowy o powierzenie grantu.
3. Umowa o powierzenie grantu zostaje zawarta w formie elektronicznej.
4. Wnioskodawca, za pośrednictwem LSI, dostarcza Partnerowi dokumenty niezbędne do zawarcia Umowy o powierzenie grantu w terminie 14 dni kalendarzowych od dnia wysłania przez Wnioskodawcę wezwania, o którym mowa w ust. 2. W przypadku niedostarczenia kompletnych co do formy i treści dokumentów w tym terminie, OOW może odstąpić od zawarcia Umowy.
5. Z uwagi na fakt, że wartość grantu musi mieścić się w limicie możliwej do udzielenia danemu Wnioskodawcy pomocy de minimis, która ustalana jest na dzień zawarcia Umowy, w przypadku, gdyby po prawidłowym złożeniu przez Wnioskodawcę dokumentów, o których mowa w ust. 4, a badanie wykazało, że kwota wskazana we Wniosku przekracza limit dozwolonej pomocy de minimis (np. w wyniku różnic kursowych), wówczas OOW odstąpi od zawarcia Umowy o powierzenie grantu. Wnioskodawca zrzeka się wobec OOW roszczeń z jakichkolwiek tytułów prawnych wynikających z niezawarcia Umowy, spowodowanego przekroczeniem, o którym mowa w zdaniu poprzednim i odstąpieniem OOW od zawarcia Umowy o powierzenie grantu.
6. W razie zaistnienia okoliczności skutkujących odstąpieniem przez którąkolwiek ze Stron od zawarcia Umowy, wybrany do wsparcia zostaje Projekt grantowy, który uzyskał następne w kolejności miejsce na liście rankingowej, o ile pozostająca kwota środków przeznaczonych na wsparcie Projektów grantowych w naborze pozwala pokryć całość wnioskowanej przez tego Wnioskodawcę kwoty wsparcia.
7. Postanowienia ust. 6 stosuje się również w sytuacji, gdy po zawarciu Umowy Wnioskodawca odstępuje od realizacji Projektu grantowego.

§ 9

Postanowienia końcowe

1. Składając Wniosek o przyznanie grantu, Wnioskodawca akceptuje warunki Konkursu Grantowego zawarte w niniejszym Regulaminie i jego załącznikach.
2. Odpowiedzi na najczęstsze pytania dotyczące Konkursu Grantowego będą publikowane w pytaniach i odpowiedziach na Stronie internetowej Konkursu.
3. Ewentualne pytania dotyczące Konkursu Grantowego Wnioskodawcy mogą zgłaszać na **adres e-mail: cyberbezpiecznewodociagi@cppc.gov.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 przepisy prawa powszechnie obowiązującego.
5. W przypadku zmiany Regulaminu, OOW zamieszcza na Stronie internetowej Konkursu 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. Kryteria wyboru Projektów grantowych;
3. Wzór Umowy o powierzenie grantu;
4. Formularz potwierdzający realną propozycję zwiększenia odporności w wyniku realizacji Projektu grantowego;
5. Zaświadczenie/Oświadczenie o otrzymanej pomocy de minimis;
6. Lista dokumentów niezbędnych do złożenia Wniosku;
7. Opis wskaźników Przedsięwzięcia pod nazwą *„Cyberbezpieczne Wodociągi”;*

8. Lista dokumentów niezbędnych do podpisania Umowy;
9. Wzór Sprawozdania z postępu rzeczowego;
10. Formularz informacji przedstawianych przy ubieganiu się o pomoc de minimis;
11. Oświadczenie o stosowaniu zasad horyzontalnych;
12. Oświadczenie o objęciu zasobów teleinformatycznych monitoringiem;
13. Instrukcja wypełnienia Wniosku w systemie LSI.