O projekcie

Nazwa projektu:
„Zwiększenie instytucjonalnej cyberodporności jednostek Państwowej Inspekcji Sanitarnej”

Projekt grantowy realizowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności Dofinansowanie ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Priorytet C3 Cyberbezpieczeństwo, Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL

Projekt realizowany na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10-CR.01-001/24/0026/KPOD.05.10-CR.01-001/25/2025 zawartego pomiędzy Centrum Projektów Polska Cyfrowa a Głównym Inspektoratem Sanitarnym

Grantobiorcą: Główny Inspektorat Sanitarny
Odbiorcy projektu: Główny Inspektorat Sanitarny oraz wszystkie graniczne stacje sanitarno-epidemiologiczne

Termin rozpoczęcia realizacji projektu: 2 lipca 2025 r.
Termin zakończenia realizacji projektu: 30 czerwca 2025 r.

Całkowita wartość realizacji projektu: 4 474 947,00 zł
Wartość dofinansowania z UE: 3 797 850,00 zł

Cel projektu grantowego
Celem projektu jest zwiększenie poziomu cyberbezpieczeństwa 10 jednostek Państwowej Inspekcji Sanitarnej – Głównego Inspektoratu Sanitarnego oraz wszystkich granicznych stacji sanitarno-epidemiologicznych:

1) **Granicznej Stacji Sanitarno-Epidemiologicznej w Dorohusku,**
2) **Granicznej Stacji Sanitarno-Epidemiologicznej w Elblągu,**
3) **Granicznej Stacji Sanitarno-Epidemiologicznej w Gdyni,**
4) **Granicznej Stacji Sanitarno-Epidemiologicznej w Hrebennem,**
5) **Granicznej Stacji Sanitarno-Epidemiologicznej w Koroszczynie,**

6) **Granicznej Stacji Sanitarno-Epidemiologicznej w Przemyślu,**
7) **Granicznej Stacji Sanitarno-Epidemiologicznej w Suwałkach,**
8) **Granicznej Stacji Sanitarno-Epidemiologicznej w Szczecinie,**
9) **Granicznej Stacji Sanitarno-Epidemiologicznej w Warszawie.**

Projekt zakłada realizację kompleksowych działań, które przyczynią się do zwiększenia instytucjonalnej cyberodporności oraz zwiększenia świadomości pracowników w zakresie bezpieczeństwa cyfrowego i zagrożeń w cyberprzestrzeni.

Główne działania zaplanowane do realizacji w 10 jednostkach Inspekcji Sanitarnej

- **przeprowadzenie audytu początkowego oraz końcowego w zakresie zgodności dokumentacji i procedur z Krajowymi Ramami Interoperacyjności/ustawą o krajowym systemie cyberbezpieczeństwa**
- **realizacja przeglądu oraz aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji**
- **zakup urządzeń i oprogramowania zwiększających odporność na cyberataki, w tym uwzględniających w szczególności zwiększenie bezpieczeństwa sieci, bezpieczeństwa styku sieci Internet z usługami wewnętrznymi, podnoszące poziom monitorowania bezpieczeństwa oraz wdrażające zarządzanie uprawnieniami użytkowników**
- **przeprowadzenie kompleksowych działań szkoleniowych podnoszących poziom świadomości pracowników w zakresie cyberbezpieczeństwa, w tym szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony oraz szkolenia specjalistyczne dla kadry zarządzającej oraz kadry istotnej z punktu widzenia wdrażanej polityki bezpieczeństwa informacji**
- **zakup dostępu do platformy edukacyjno-szkoleniowej umożliwiającej symulację cyberataków oraz przygotowanie dedykowanych modułów szkoleniowych w zakresie bezpieczeństwa cyfrowego i cyberhigieny**
- **przygotowanie periodyków i newsletter informujących o cyberzagrożeniach oraz działaniach minimalizujących podatność na ataki w cyberprzestrzeni**

Zgodność projektu z wypracowanymi w ramach Państwowej Inspekcji Sanitarnej standardami cyberbezpieczeństwa

Zaplanowane w ramach projektu działania odzwierciedlają wdrażane w Państwowej Inspekcji Sanitarnej standardy cyberbezpieczeństwa definiujące cztery poziomy instytucjonalnej cyberodporności: rozwiązania kopii zapasowych, rozwój systemów bezpieczeństwa sieci oraz bezpieczeństwa styku sieci Internet z usługami wewnętrznymi, bezpieczeństwo poczty elektronicznej oraz rozwój systemów monitorowania bezpieczeństwa i reagowania.