



Projekt Cyberbezpieczny Samorząd

WOJCIECH PUKSZTA
KOORDYNATOR PROJEKTU

e-mail: wp@cyber-samorzad.pl

tel.: 698 371 001

<https://cyber-samorzad.pl>

Agenda oferty

01. Projekt Cyberbezpieczny Samorząd

Cel Projektu

02. Projekt Cyberbezpieczny Samorząd

Cel Projektu - obszary wydatków

03. Projekt Cyberbezpieczny Samorząd

Nasza pomoc w uzyskaniu grantu

04. Projekt Cyberbezpieczny Samorząd

Kto, Gdzie, Kiedy

05. Projekt Cyberbezpieczny Samorząd

Harmonogram - Oś czasu

Agenda oferty

- 06. Projekt Cyberbezpieczny Samorząd
Budżet Projektu
- 07. Projekt Cyberbezpieczny Samorząd
Nasi klienci
- 08. Projekt Cyberbezpieczny Samorząd
O nas

Cel Projektu

- zwiększenie poziomu cyfryzacji Jednostek Samorządu Terytorialnego;
- zwiększenie poziomu odporności na cyberzagrożenia systemów teleinformatycznych;
- zapewnienie podstawowych atrybutów bezpieczeństwa przetwarzanym przez JST danym tj. poufność, dostępność i integralność;
- prowadzenie monitoringu zdarzeń w systemach teleinformatycznych w trybie ciągłym przy wykorzystaniu systemów klasy SIEM;
- zapewnienie ciągłości działania JST w zgodzie z zapisami normy ISO 22301.



Projekt Cyberbezpieczny Samorząd

NA JAKI CEL MOŻNA PRZEZNACZYĆ GRANTY

01

OBSZAR KOMPETENCYJNY:

1. Podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST.
2. Szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.
3. Szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa.
4. Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

02

OBSZAR TECHNICZNY:

1. Zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta.
2. Zakup, wdrożenie i utrzymanie rozwiązań ciągłego monitorowania bezpieczeństwa (skanery podatności, zarządzanie podatnościami, zarządzanie zasobami IT i aktywami podlegającymi ochronie).
3. Zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania.
4. Zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa.
5. Zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC, ang. Security Operations Centre), także jako element Centrum Usług Wspólnych,
6. Zakup testów i badań bezpieczeństwa, dostępu do usług rozpoznawania zagrożeń w cyberprzestrzeni – CTI (ang. Cyber Threat Intelligence), dostępu do informacji bezpieczeństwa oraz innych usług integracyjnych dotyczących obszaru cyberbezpieczeństwa.

03

OBSZAR ORGANIZACYJNY

1. Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
2. Audyt SZBI, audyt zgodności z wymaganiami KRI / uoKSC przez wykwalifikowanych audytorów, (re)certyfikacja SZBI na zgodność z normami.
3. Wprowadzenie lub aktualizacja Polityk Bezpieczeństwa Informacji (PBI), analiza ryzyka (w tym opracowanie i wdrożenie metodyk), opracowanie procedur: obsługi incydentów, ciągłości działania i zarządzania kryzysowego, stosowania kryptografii, kontroli dostępu, bezpieczeństwa pracy zdalnej, używania urządzeń mobilnych itp.

Projekt Cyberbezpieczny Samorząd

JAKICH WYDATKÓW NIE ROZLICZYSZ W RAMACH PROJEKTU

DO WSPÓŁFINANSOWANIA NIE KWALIFIKUJĄ SIĘ WSZELKIE WYDATKI NA ZAKUP, DOSTAWĘ LUB USŁUGI, KTÓRE NIE SŁUŻĄ BEZPOŚREDNIO WSPARCIU CYBERBEZPIECZEŃSTWA W JST, W SZCZEGÓLNOŚCI:

- Stacje robocze lub laptopy;
- Urządzenia mobilne tj. smartfony lub tablety;
- Akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, klawiatury, myszy);
- Materiały eksploatacyjne;
- Oprogramowanie biurowe, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;
- Szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;
- Usługi dostępu do internetu, abonamenty telefoniczne.

Projekt Cyberbezpieczny Samorząd

ROLA NASZYCH EKSPERTÓW W PROJEKCIE

MOŻESZ LICZYĆ NA NASZE WSPARCIE NA KAŻDYM ETAPIE REALIZACJI PROJEKTU.
DZIĘKI NASZEJ POMOCY PAŃSTWA SAMORZĄD

- Jednostka Samorządu Terytorialnego (JST) zyskuje profesjonalną ocenę stanu systemów teleinformatycznych, bazującą na solidnych wnioskach KRI i współpracy z doświadczonym Zespołem IT.
- Otrzymuje dokładną analizę procesów, które są w pełni zgodne z Polityką Bezpieczeństwa Informacji oraz obowiązkami KRI, co gwarantuje zgodność z najwyższymi standardami.
- Zapewniamy rzetelną weryfikację analiz ryzyka, skupiając się na nadzorze procesów krytycznych, zgodnie z Narodowymi Standardami Cyberbezpieczeństwa.
- Jesteśmy wsparciem w procesie składania wniosków o udział w projekcie "Cyberbezpieczny samorząd".
- Pomagamy w przygotowaniu Ankiety dotyczącej cyberdojrzałości, która precyzyjnie określa potrzeby JST w kluczowych obszarach: technicznym, kompetencyjnym i organizacyjnym.

Projekt Cyberbezpieczny Samorząd

ROLA NASZYCH EKSPERTÓW W PROJEKCIE

MOŻESZ LICZYĆ NA NASZE WSPARCIE NA KAŻDYM ETAPIE REALIZACJI PROJEKTU.
DZIĘKI NASZEJ POMOCY PAŃSTWA SAMORZĄD - CD

- Realizujemy dla Państwa wszystkie czynności wynikające z umowy, w tym budowę SZBI oraz przeprowadzenie audytów KRI.
- W razie potrzeby służymy wsparciem w zakupie nowoczesnego sprzętu IT oraz licencji, gwarantując najlepsze rozwiązania na rynku.
- Przygotowujemy drugą Ankietę dotyczącą cyberdojrzałości, która wskazuje na wzrost poziomu cyberbezpieczeństwa JST, dzięki efektywnemu wydatkowaniu otrzymanego grantu.
- Jesteśmy niezastąpioną pomocą w procesie przygotowania i rozliczenia otrzymanego grantu, dzięki czemu JST może skupić się na swoich kluczowych zadaniach.

Projekt Cyberbezpieczny Samorząd

KTO, GDZIE, KIEDY

Do projektu przystępują Jednostki Samorządu Terytorialnego na każdym poziomie przy wyłączeniu placówek zdrowia. Pozyskane środki mogą posłużyć również do wsparcia Jednostek podległych, podnosząc tym samym poziom ogólnego cyberbezpieczeństwa.

01

KTO

Łączna ilość - 2807 JST

- Gminy - 2 477
- Powiaty - 314
- Województwa - 16

02

GDZIE

Oficjalna rządowa strona
Projektu:

https://www.gov.pl/web/cp_pc/cyberbezpieczny-samorzad

03

KIEDY

Termin składania wniosków
upływa 30.11.2023 o
godzinie 16:00

Oś czasu Projektu

19.07.2023

30.11.2023

+ 60 DNI

+ 30 DNI

MAX. 24 M-CE

START PROJEKTU

Od tego dnia wszystkie JST mogą składać wnioski. Zaleca się, aby na tym etapie uczestniczył w JST Zespół ds. Systemu Zarządzania Bezpieczeństwem Informacji.

TUTAJ UZYSKASZ NASZE
WSPARCIE

ZAMKNIĘCIE WNISKOWANIA

Pierwotny termin końca składania wniosków został wydłużony. Aktualny termin mija 30.11.2023 o godzinie 16:00

OCENA WNIOSKU I PODPISANIE UMOWY

Ocena wniosku trwa około 60 dni, liczonych od dnia złożenia wniosku. W przypadku błędu, JST będzie miało 3 dni robocze na poprawę wniosku. Potem następuje podpisanie umowy o powierzenie grantu.

TUTAJ UZYSKASZ NASZE
WSPARCIE

DOSTARCZENIE ANKIETY

Do 30 dni po podpisaniu umowy, JST zobowiązane jest dostarczyć Ankiętę Dojrzałości Cyberbezpieczeństwa w JST.

TUTAJ UZYSKASZ NASZE
WSPARCIE

AUDYT KRI

Obowiązkowo, przed rozliczeniem grantu, JST zobowiązane jest przeprowadzić obowiązkowy Audyt KRI. Audyt jest kosztem kwalifikowanym.

TUTAJ UZYSKASZ NASZE
WSPARCIE

KONIEC PROJEKTU

Okres realizacji Projektu Grantowego i jego rozliczenie wynosi maksymalnie 24 miesiące od dnia wejścia w życie Umowy o powierzenie Grantu, jednak nie później niż do 30.06.2026 r.

TUTAJ UZYSKASZ NASZE
WSPARCIE

Budżet Projektu

BUDŻET CAŁEGO PROJEKTU



1.8 MLD ZŁ

Łączna kwota przeznaczona
na Projekt to prawie 2 MLD zł.

PODZIAŁ BUDŻETU NA JST

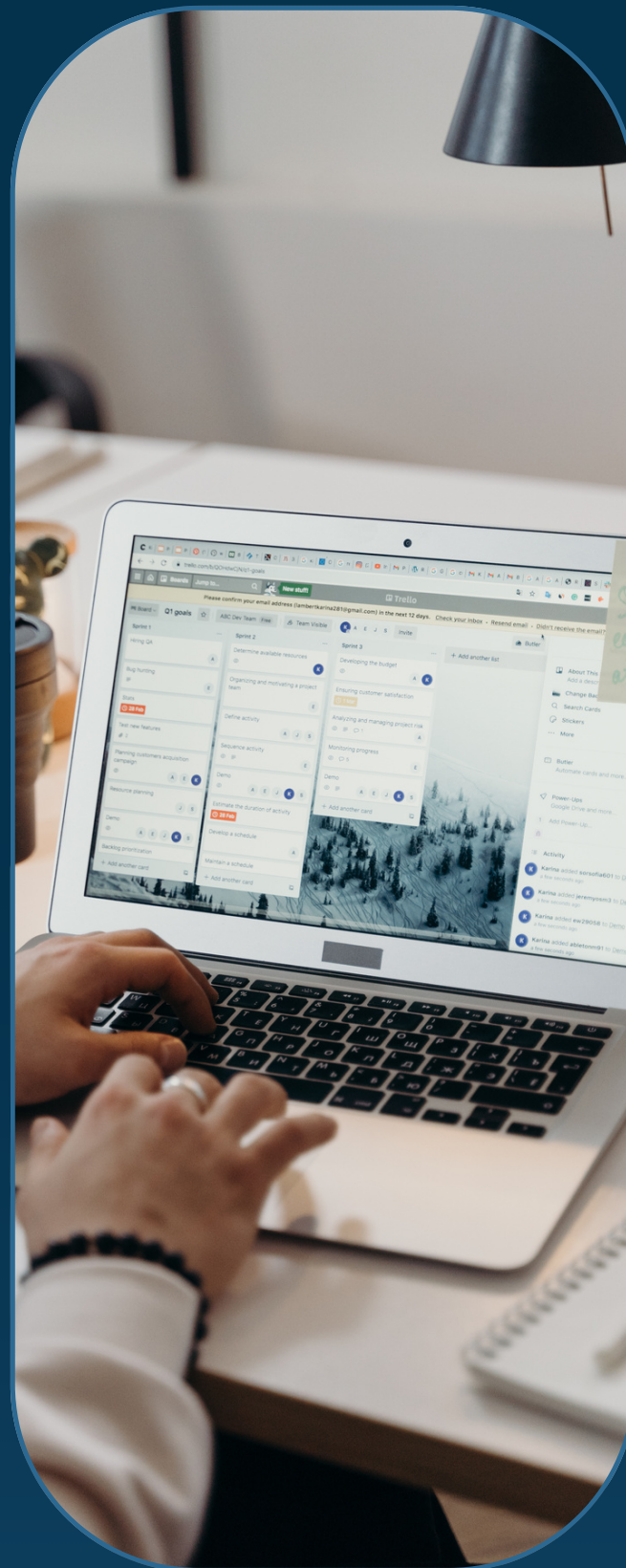


MAX. 0.85 MLN

- Gminy: 200.000 do 850.000
- Powiaty: do 850.000
- Województwa: do 850.000

Nasi klienci

Nasi klienci to nowoczesne firmy i instytucje, które rozumieją znaczenie innowacji i bezpieczeństwa w dzisiejszym cyfrowym świecie. Wybierają nasze usługi, ponieważ cenią sobie profesjonalizm, indywidualne podejście oraz skuteczność w działaniu. Doceniają naszą zdolność do dostosowywania się do ich unikalnych potrzeb oraz nasze zaangażowanie w dostarczanie rozwiązań najwyższej jakości. Dla wielu z nich jesteśmy nie tylko dostawcą usług, ale przede wszystkim zaufanym partnerem w biznesie.





O nas

O NASZEJ FIMIE I AUDITORACH

Jesteśmy zespołem, specjalizującym się w ochronie danych osobowych i bezpieczeństwie informacji. Współpracujemy z ekspertami w dziedzinie cyberbezpieczeństwa i informatyki śledczej. Posiadamy certyfikaty z zakresu bezpieczeństwa informacji, w tym Audytora Wiodącego ISO 27001 z akredytacją IRCA oraz certyfikaty wydane przez ABW i TUV Nord. Aktywnie uczestniczymy w konsultacjach z Urzędem Ochrony Danych Osobowych i współpracujemy z Ministerstwem Cyfryzacji.

[więcej o nas- kliknij](#)

Dziękujemy i zapraszamy do współpracy

Wybierając naszą firmę, Jednostka Samorządu Terytorialnego inwestuje w przyszłość, bezpieczeństwo i profesjonalizm.

Zapewniamy kompleksowe wsparcie na każdym etapie współpracy w Projekcie Cyberbezpieczny Samorząd.

INSPEKTORZYRODO.PL SP. Z O.O.

00-682 Warszawa ul. Hoża 86/410

e-mail: kontakt@cyber-samorzad.pl

tel.: +48 577 779 296

<https://cyber-samorzad.pl>