Regulamin Konkursu Grantowego pn. "Cyberbezpieczny Samorząd"

1. Grantodawca przyzna Grantobiorcy Grant na zadania w ramach poniżej wskazanych obszarów:

   1) **obszar organizacyjny** - środki można przeznaczyć na następujące działania (usługi):
      a) opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym między innymi wprowadzenie lub aktualizacja polityk bezpieczeństwa informacji (PBI), na analizy ryzyka (w tym opracowanie i wdrożenie metodyk), np. procedury: obsługi incydentów, ciągłości działania i zarządzania kryzysowego, stosowania kryptografii i szyfrowania, kontroli dostępu, bezpieczeństwa pracy zdalnej, używania urządzeń mobilnych, itp.,
      b) audyt SZBI, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów, (re-)certyfikacja SZBI na zgodność z normami;
   2) **obszar kompetencyjny** - środki można przeznaczyć na następujące działania (usługi):
      a) podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST,
      b) szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji,
      c) szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu,
      d) 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;
   3) **obszar techniczny** - 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.

2. Grantobiorca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247), zwanego dalej „rozporządzeniem KRI"

1. Do wydatków kwalifikowanych w ramach Grantu zalicza się w szczególności:
   1) środki trwałe/dostawy:
      a) sprzęt informatyczny i Urządzenia bezpieczeństwa:
         - Firewall sieciowy;
         - WAF (Web Application Firewall);
         - SIEM (Security Information and Event Management);
         - UTM (Unified Threat Management);
         - IPS (Intrusion Prevention System);
         - IDS (Intrusion Detection System);
         - VPN (Virtual Private Network);
         - NAC (Network Access Control); proxy sprzętowe; serwer;
         - serwer do wykonywania kopii zapasowych;
         - macierz dyskowa;
         - dyski twarde do macierzy dyskowej;
         - Network Attached Storage (NAS); Storage Area Network (SAN); Web Secure Gateway;
         - Email Secure Gateway;
         - generator prądu; UPS;
         - ochrona AntyDDoS;
         - zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X;
   2) wartości niematerialne i prawne, w szczególności:
      a) wartości niematerialne i prawne, takie jak: autorskie prawa majątkowe lub licencje, w tym subskrypcyjne, na korzystanie z oprogramowania, w tym systemowego o przewidywanym okresie używania dłuższym niż rok; prawa do dokumentacji, raportów, opracowań. Koszty kwalifikowane będą tylko w okresie realizacji Projektu:
         - oprogramowanie antywirusowe;
         - oprogramowanie typu EDR (Endpoint Detection and Response);
         - oprogramowanie typu XDR (Extended Detection and Response);
         - oprogramowanie do wykonywania kopii zapasowych;
         - oprogramowanie antyspamowe;
         - oprogramowanie WAF (Web Application Firewall);
         - oprogramowanie SIEM (Security Information and Event Management);
         - oprogramowanie Menadżera logów;
         - oprogramowanie do zarządzania podatnościami;

- programowanie przeciwdziałającemu wyciekowi danych (DLP – Data Leak Prevention);
- oprogramowanie do zarządzania uprzywilejowanemu dostępowi (PAM- Privileged Access Management);
- oprogramowanie Web Secure Gateway;
- oprogramowanie Email Secure Gateway;
- oprogramowanie do zarządzania tożsamością i dostępem;
- oprogramowanie centralnego menadżera haseł;
- oprogramowanie do monitorowania infrastruktury informatycznej;
- oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych;
- oprogramowanie do badania podatności systemów informatycznych;
- oprogramowanie do badania podatności serwisów WWW;
- oprogramowanie do badania podatności w kodzie aplikacji;
- oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików;
- oprogramowanie do analizy po włamaniowej;
- oprogramowanie do ochrony przed ransomware;

3) usługi zewnętrzne, w szczególności:
   a) przygotowanie Projektu: sfinansowanie przygotowania Projektu opracowanego przez specjalistów / organizacje, w których osoba odpowiedzialna za przygotowania Projektu posiada stosowną wiedzę i m.in. 2 letnie doświadczenie we wnioskowanym zakresie oraz co najmniej 1 (jeden) certyfikat świadczący o posiadanej wiedzy w danym zakresie. Koszty będą kwalifikowane tylko w okresie realizacji projektu;
   b) usługi informatyczne. Pokrycie kosztów zwiększających poziom bezpieczeństwa informacji, tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych tylko w okresie realizacji Projektu:
      - usługa poczty elektronicznej w chmurze obliczeniowej typu IaaS, SaaS, PaaS z elementami bezpieczeństwa;
      - usługa testowania bezpieczeństwa infrastruktury sieciowej;
      - usługa testowania bezpieczeństwa serwisów internetowych;
      - usługa testowania bezpieczeństwa aplikacji;
      - usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS w zakresie sandbox do badania bezpieczeństwa aplikacji oraz plików;
      - usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego;
   c) usługi wspomagające realizację Projektu, w szczególności usługi doradcze podmiotów posiadających stosowne kwalifikacje i min. 2 letnim doświadczeniem w prowadzeniu projektów z obszaru cyberbezpieczeństwa oraz stosowne certyfikaty lub równoważne poświadczenia (np. Kwalifikację zawodową) potwierdzające możliwość wykonania zlecenia. Kwalifikowalność kosztów tylko w okresie realizacji Projektu;
   d) szkolenia: zakup i organizacja szkoleń stacjonarnych lub/ i online dedykowanych dla

pracowników JST zorganizowanych przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. Kwalifikowalność kosztów tylko w okresie realizacji Projektu;

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

2. **Do wydatków niekwalifikowalnych w ramach Grantu zaliczają się:**
   1) do współfinansowania nie kwalifikują się wszelkie wydatki określone w podrozdziale 3.3. Katalogu wydatków kwalifikowanych II priorytetu programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027;
   2) do współfinansowania nie kwalifikują się wszelkie wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa w JST, w szczególności:
      a) komputery stacjonarne i przenośne;
      b) urządzenia mobilne tj. smartfony lub tablety;
      c) akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, klawiatury, myszy);
      d) materiały eksploatacyjne;
      e) oprogramowanie biurowe, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;
      f) szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;
      g) usługi dostępu do internetu, abonamenty telefoniczne.