Regulamin Konkursu Grantowego

Cyberbezpieczny Samorząd - fragment

Priorytet II: Zaawansowane usługi cyfrowe

Warszawa, lipiec 2023 r.

1. Dofinansowanie udzielane w formie grantów może być przeznaczone na zadania w ramach poniżej wskazanych obszarów:

1.		Obszar organizacyjny	Środki można przeznaczyć na następujące działania (usługi): • 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. • 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): • podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST, • szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji, • szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach projektu grantowego, • 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): • zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta, • 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, • zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i

		oprogramowania z zakresu cyberbezpieczeństwa, • zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa, • zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych, • 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", zgodnie z poniższymi warunkami: ...