

Załącznik nr 4 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Wykonanie audytu bezpieczeństwa informacji i cyberbezpieczeństwa zgodnie z wymaganiami normy PN ISO/IEC 27001:2023 oraz wymaganiami prawnymi w zakresie KRI oraz ustawy o krajowym systemie cyberbezpieczeństwa dla urzędu gminy Gójnik i jednostki podległej Gminny Ośrodek Pomocy Społecznej

ZAMAWIAJĄCY

Urząd Gminy Gójnik jest urzędem administracji samorządowej, obsługującym lokalną społeczność zgodnie z zakresem prawnym określonym w Ustawie z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2024 r. poz. 609) i realizuje zadania zlecone przez administrację rządową. Urząd kieruje się przede wszystkim dobrem mieszkańców gminy, a jej głównym celem jest realizacja zadań i podejmowanie działań na rzecz tych mieszkańców określone w przepisach prawa.

W związku z powyższym Zamawiający realizuje projekt grantowy pn. *Wzmocnienie odporności cyfrowej w Gminie Gójnik*, którego celem jest poprawa jakości bezpieczeństwa usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji w kontekście zwiększenia poziomu cyberbezpieczeństwa.

Urząd Gminy w Gójniku zatrudnia 46 osób. Regulamin organizacyjny oraz schemat znajdują na stronie internetowej urzędu pod wskazanym adresem internetowym:

- <https://bip.malopolska.pl/uggnojnik,m,76160,struktura-urzedu.html>
- <https://bip.malopolska.pl/uggnojnik,m,76166,regulamin-organizacyjny-urzedu.html>

Jednostka organizacyjna Gminnym Ośrodkiem Pomocy Społecznej w Gójniku zatrudnia 10 osób. Regulamin organizacyjny oraz schemat znajdują na stronie internetowej urzędu pod wskazanym adresem internetowym:

- <https://gnojnik.naszops.pl/statut>
- <https://bip.malopolska.pl/gopspolecznej,m,237730,struktura-organizacyjna.html>

Urząd posiada następującą ilość sprzętu IT:

1. Stanowiska komputerowe (hosty): 47 (+9 laptopów do pracy zdalnej)
2. Serwery fizyczne i urządzenia macierzowe: 7
3. Urządzenie sieciowe wewnętrzne: 9
4. Urządzenie na styku sieci LAN/WAN (Internet): 2 (oraz infrastruktura PL.id)

GOPS posiada następującą ilość sprzętu IT:

1. Stanowiska komputerowe (hosty): 10
2. Serwery i urządzenia macierzowe: infrastruktura UG

3. Urządzenie sieciowe wewnętrzne: infrastruktura UG
4. Urządzenie na styku sieci LAN/WAN (Internet): infrastruktura UG

Dodatkowe informacje w postaci adresaci sieci lub inne uzupełniające, Zamawiający przekaze po podpisaniu umowy.

PRZEDMIOT ZAMÓWIENIA

Usługa

Przedmiotem zamówienia jest wykonanie audyt bezpieczeństwa informacji i cyberbezpieczeństwa zgodnie z wymagania normy PN ISO/IEC 27001:2023 oraz wymagań prawnych w zakresie KRI oraz ustawy o krajowym systemie cyberbezpieczeństwa w zakresie organizacyjnym i technicznym.

CPV: 79417000-0 Usługi doradcze w zakresie bezpieczeństwa

CPV: 79212000-3 Usługi audytu

TERMIN REALIZACJI USŁUGI

Realizacja audytu w ciągu 14 dni od podpisania umowy. Raport z audytu w ciągu 14 dni od zakończenia audytu.

Realizacja usługi zostanie potwierdzona protokołem końcowym odbioru.

SZCZEGÓŁOWY ZAKRES ZAMÓWIENIA

Audyt przeprowadzony będzie w zakresie dwóch czynności audytowych:

1. Audyt Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o wymagania normy PN EN ISO/IEC 27001:2023, w tym wymogów przepisów prawa w zakresie KRI i cyberbezpieczeństwa, oceny środków kontroli w zakresie bezpieczeństwa informacji zgodnie z ISO/IEC TS 27008:2019. Audyt wykonany ma być zgodnie z wymaganiami przeprowadzania audytów ISO 19011:2018. Wynikiem audytu ma być raport niezgodności, wraz ze wskazówkami, jakie czynności należy podjąć w celu ich niwelowania.
2. Audyt podatności, którego celem jest skanowanie podatności systemów informatycznych i wskazanie podatności oraz zagrożeń, w tym ich identyfikacja i działań jakie należy podjąć w celu ich wyeliminowania. Audyt podatności ma zapewnić wykrywanie podatności, błędnych konfiguracji i problemów ze zgodnością w sieciach, aplikacjach internetowych. Zamawiający otrzyma raport wraz z czynnościami jakie należy podjąć w celu niwelowania podatności. Raport powinien określać poziom ryzyka jaką dana podatność może wpływać na daną infrastrukturę IT.
Minimalny zakres narzędzie do skanowania podatności:
 - a. Wykrywanie wiele rodzajów podatności, np. przestarzałe systemy i oprogramowanie, błędy konfiguracji, słabe hasła, niezabezpieczone dane osobowe, słabe szyfrowanie i złośliwe oprogramowanie.

- b. Skanowanie infrastruktury, w tym systemy lokalne, komputery pracowników w biurze i zdalnych, urządzenia sieciowe.
- c. Skanowanie uwierzytelnione, jak i niewierzytelnione.
- d. Wspieranie skanowanie polityk pod kątem benchmarków CIS.
- e. Podatności mają być identyfikowane i porównywane z bazą znanych podatności (CVE).
- f. Skanowanie ma być oparte o rozwiązanie chmurowe z możliwością instalacji klienta skanowania w infrastrukturze IT lub dostarczenie gotowego rozwiązania IT w zakresie skanowania podatności w infrastrukturze Zamawiającego.
- g. Skanowanie aplikacji internetowych (serwisów internetowych)

REALIZACJA USŁUGI

1. W ramach usługi Wykonawca przeprowadzi przynajmniej jedno spotkanie w siedzibie Zamawiającego.
2. Wszystkie dokumenty sporządzone będą w formie pisemnej w języku polskim, w formie papierowej oraz formie elektronicznej w formacie danych .pdf oraz jednym z formatów edytowalnych: .docx, .rtf, .xlsx. Wszelkie dane przekazywane w sposób elektroniczny (w tym za pomocą środków komunikacji elektronicznej) powinny być w sposób odpowiedni zabezpieczony, uniemożliwiający tym samym dostęp osobom postronnym.
3. Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty niniejszego zamówienia.
4. Informacje, które będą przekazywane w celu realizacji usługi, stanowią informacje chronione, w związku z tym realizacja projektu będzie wymagała akceptacji zapisów o zachowaniu poufności i zapewnieniu stosownej ochrony, w tym również dla danych osobowych. Zasady dotyczące poufności w tym ochrony danych osobowych zostaną przyjęte przez obie strony w formie pisemnej w momencie zawarcia umowy na realizację usług.