

**Ogłoszenie o wyniku postępowania
Usługi****„Usługa wykonania audytu systemu bezpieczeństwa informacji w 5 podmiotach w ramach projektu „Cyberbezpieczny samorząd dla Gminy Stalowa Wola”****SEKCJA I - ZAMAWIAJĄCY****1.1.) Rola zamawiającego**

Postępowanie prowadzi zamawiający centralny

1.2.) Nazwa zamawiającego: Stalowowolskie Centrum Usług Wspólnych**1.4) Krajowy Numer Identyfikacyjny:** REGON 384503002**1.5) Adres zamawiającego****1.5.1.) Ulica:** Al. Jana Pawła II 25A**1.5.2.) Miejscowość:** Stalowa Wola**1.5.3.) Kod pocztowy:** 37-450**1.5.4.) Województwo:** podkarpackie**1.5.5.) Kraj:** Polska**1.5.6.) Lokalizacja NUTS 3:** PL824 - Tarnobrzeski**1.5.9.) Adres poczty elektronicznej:** zp@stalowawola.pl**1.5.10.) Adres strony internetowej zamawiającego:** <https://bip.stalowawola.pl/?c=mdTresc-cmPokaz-1657>**1.6.) Adres strony internetowej prowadzonego postępowania:**<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-3777d561-6d63-4db9-ac22-fad52e2f89c8>**1.7.) Rodzaj zamawiającego:** Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka budżetowa**1.8.) Przedmiot działalności zamawiającego:** Ogólne usługi publiczne**SEKCJA II – INFORMACJE PODSTAWOWE****2.1.) Ogłoszenie dotyczy:**

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie**2.3.) Nazwa zamówienia albo umowy ramowej:**

„Usługa wykonania audytu systemu bezpieczeństwa informacji w 5 podmiotach w ramach projektu „Cyberbezpieczny samorząd dla Gminy Stalowa Wola”

2.4.) Identyfikator postępowania: ocds-148610-3777d561-6d63-4db9-ac22-fad52e2f89c8**2.5.) Numer ogłoszenia:** 2026/BZP 00272172**2.6.) Wersja ogłoszenia:** 01**2.7.) Data ogłoszenia:** 2026-06-02**2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań:** Nie**2.11.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej:** Tak**2.12.) Nazwa projektu lub programu:**

Zadanie jest dofinansowane w ramach Programu: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027. Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa.

2.13.) Zamówienie/umowa ramowa było poprzedzone ogłoszeniem o zamówieniu/ogłoszeniem o zamiarze zawarcia umowy: Tak**2.14.) Numer ogłoszenia:** 2026/BZP 00209292**SEKCJA III – TRYB UDZIELENIA ZAMÓWIENIA LUB ZAWARCIA UMOWY RAMOWEJ**

3.1.) Tryb udzielenia zamówienia wraz z podstawą prawną Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Numer referencyjny: ZP-III.261.108.2026.MJ

4.2.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Tak

4.3.1) Wartość zamówienia stanowiącego przedmiot tego postępowania (bez VAT): 48780,49 PLN

4.4.) Rodzaj zamówienia: Usługi

4.5.1.) Krótki opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest „Usługa wykonania audytu systemu bezpieczeństwa informacji w 5 podmiotach w ramach projektu „Cyberbezpieczny samorząd dla Gminy Stalowa Wola”: Zaawansowane usługi cyfrowe Działanie 2.2- Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”
Zamówienie obejmuje przeprowadzenie audytów systemu bezpieczeństwa informacji w 5 podmiotach:

- Urzędzie Miasta w Stalowej Woli
- Żłobku Miejskim Nr 3 w Stalowej Woli,
- Przedszkolu Nr 2 im. Jana Brzechwy w Stalowej Woli
- Przedszkolu Nr 5 im. Juliana Tuwima w Stalowej Woli
- Stalowowskim Centrum Usług Wspólnych

mi.in. w celu oceny skuteczności środków bezpieczeństwa oraz zarządzania ryzykiem;

- a) audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI,
- b) analizę efektywności działań w zakresie monitorowania, pomiarów, analizy i oceny SZBI, w tym przegląd wskaźników ryzyka i zgodności.

Zadanie jest dofinansowane w ramach Programu: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027. Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa.

2. AUDYT POWINIEN OBEJMOWAĆ:

a) Analiza wstępną i określenie zakresu audytu

- Zdefiniowanie obszarów, lokalizacji oraz jednostek organizacyjnych objętych SZBI.
- Weryfikacja ewidencji obszaru przetwarzania informacji, w tym dokładność danych dotyczących lokalizacji, kondygnacji i adresów.
- Sprawdzenie, czy zakres SZBI jest zgodny z wymaganiami norm ISO/IEC 27001 oraz potrzebami organizacji.

b) Weryfikacja dokumentacji systemowej

- Wprowadzenie do SZBI: Ocena, czy dokumentacja zawiera podstawowe zasady zarządzania bezpieczeństwem informacji i zgodność z cyklem PDCA (Plan-Do-Check-Act).
- Terminy i definicje: Sprawdzenie, czy wszystkie istotne pojęcia są zdefiniowane i zgodne z normami.
- Kontekst organizacji: Analiza czynników wewnętrznych i zewnętrznych oraz ich wpływu na SZBI, w tym analiza ryzyk.

c) Zarządzanie ryzykiem

- Ocena procesu identyfikacji i analizy ryzyk, w tym dokumentacji dotyczącej szacowania ryzyk.
- Analiza działań zaradczych i korygujących dla zidentyfikowanych ryzyk.

d) Zabezpieczenia i deklaracja stosowania

- Weryfikacja, czy deklaracja stosowania zabezpieczeń jest zgodna z Załącznikiem A normy ISO/IEC 27001.
- Ocena skuteczności wdrożonych zabezpieczeń oraz uzasadnienia ewentualnych wyłączeń.

e) Dokumentacja operacyjna

- Polityki i procedury: Sprawdzenie polityk bezpieczeństwa (np. kryptografii, zarządzania dostępem, bezpieczeństwa zasobów ludzkich) i ich zgodności z wymaganiami normatywnymi.
- Ewidencje i rejestry: Ocena kompletności i aktualności ewidencji aktywów, obszarów przetwarzania informacji oraz rejestrów incydentów i zgłoszeń
- Zarządzanie dostępem: Sprawdzenie procedur przyznawania, zmiany i odbierania dostępu oraz zgodności z dokumentacją.

f) Monitorowanie i doskonalenie SZBI

- Ocena procesów monitorowania, analizy i oceny systemu w odniesieniu do zgodności z wymaganiami i celami bezpieczeństwa.
- Weryfikacja raportów z monitorowania, przeglądów zarządzania i działań korygujących.
- Analiza działań doskonalących, w tym ocena skuteczności realizowanych zmian.

g) Zarządzanie incydentami i ciągłością działania

- Ocena polityki zarządzania incydentami, w tym procedur zgłaszania, oceny i reagowania na incydenty.
- Sprawdzenie planów zarządzania ciągłością działania i odtwarzania po katastrofie, w tym testów i analiz RTO, RPO, MTPD i MBCO.

h) Audyty wewnętrzne

- Weryfikacja programu i planów audytów wewnętrznych, w tym ocena zgodności z wymaganiami ISO/IEC 27001.
- Sprawdzenie raportów z audytów wewnętrznych pod kątem ustaleń, zgodności i zaleceń.

i) Zgodność z przepisami i ochroną danych osobowych

- Ocena dokumentacji dotyczącej przetwarzania danych osobowych, w tym zgodności z RODO.
- Weryfikacja rejestrów czynności przetwarzania danych, ocen skutków dla ochrony danych oraz testów równowagi.

j) Dokumentacja operacyjna

- Analiza polityk i procedur dotyczących korzystania z systemów, urządzeń i sieci.
- Weryfikacja zasad postępowania z nośnikami informacji, tworzenia haseł i korzystania z Internetu oraz poczty elektronicznej.

k) Zarządzanie dostawcami

- Sprawdzenie polityk i procedur związanych z bezpieczeństwem informacji w relacjach z dostawcami.
- Ocena zgodności działań dostawców z wymaganiami organizacji.

l) Zgodność z wymaganiami prawnymi

- Weryfikacja dokumentacji dotyczącej monitorowania i przestrzegania wymagań prawnych, regulacyjnych i umownych.
- Analiza zgodności z politykami zgodności oraz audytami technicznymi.

4.5.3.) Główny kod CPV: 72800000-8 - Usługi audytu komputerowego i testowania komputerów

4.5.4.) Dodatkowy kod CPV:

72810000-1 - Usługi audytu komputerowego

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się zawarciem umowy

SEKCJA VI OFERTY

6.1.) Liczba otrzymanych ofert lub wniosków: 9

6.1.1.) Liczba otrzymanych ofert wariantowych: 0

6.1.2.) Liczba ofert dodatkowych: 0

6.1.3.) Liczba otrzymanych od MŚP: 9

6.1.4.) Liczba ofert wykonawców z siedzibą w państwach EOG innych niż państwo zamawiającego: 0

6.1.5.) Liczba ofert wykonawców z siedzibą w państwie spoza EOG: 0

6.1.6.) Liczba ofert odrzuconych, w tym liczba ofert zawierających rażąco niską cenę lub koszt: 4

6.1.7.) Liczba ofert zawierających rażąco niską cenę lub koszt: 6

6.2.) Cena lub koszt oferty z najniższą ceną lub kosztem: 15990,00 PLN

6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 52000,00 PLN

6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 36198,90 PLN

6.5.) Do wyboru najkorzystniejszej oferty zastosowano aukcję elektroniczną: Nie

6.6.) Oferta wybranego wykonawcy jest ofertą wariantową: Nie

SEKCJA VII WYKONAWCA, KTÓREMU UDZIELONO ZAMÓWIENIA

7.1.) Czy zamówienie zostało udzielone wykonawcom wspólnie ubiegającym się o udzielenie zamówienia: Nie

7.2.) Wielkość przedsiębiorstwa wykonawcy: Mikro przedsiębiorca

7.3.) Dane (firmy) wykonawcy, któremu udzielono zamówienia:

7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia: AGILEO IT Sp. z o.o.

7.3.2) Krajowy Numer Identyfikacyjny: REGON 243108344

7.3.3) Ulica: Konarskiego 18C

7.3.4) Miejscowość: Gliwice

7.3.5) Kod pocztowy: 44-100

7.3.6.) Województwo: śląskie

7.3.7.) Kraj: Polska

7.4.) Czy wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcom?: Nie

SEKCJA VIII UMOWA

8.1.) Data zawarcia umowy: 2026-05-15

8.2.) Wartość umowy/umowy ramowej: 36198,90 PLN

8.3.) Okres realizacji zamówienia albo umowy ramowej:
do 2026-05-25