

**Ogłoszenie o wyniku postępowania
Dostawy
Poprawa cyberbezpieczeństwa w Gminie Jaraczewo**

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: GMINA JARACZEWO

1.4) Krajowy Numer Identyfikacyjny: REGON 250855363

1.5) Adres zamawiającego

1.5.1.) Ulica: ul. Jarocińska 1

1.5.2.) Miejscowość: Jaraczewo

1.5.3.) Kod pocztowy: 63-233

1.5.4.) Województwo: wielkopolskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL416 - Kaliski

1.5.7.) Numer telefonu: 62 747 31 02

1.5.8.) Numer faksu: 62 747 31 02

1.5.9.) Adres poczty elektronicznej: ug@jaraczewo.pl

1.5.10.) Adres strony internetowej zamawiającego: www.jaraczewo.pl

1.6.) Adres strony internetowej prowadzonego postępowania:

<https://platformazakupowa.pl/transakcja/1144105>

1.7.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

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:

Poprawa cyberbezpieczeństwa w Gminie Jaraczewo

2.4.) Identyfikator postępowania: ocds-148610-d42aa43c-b276-4435-8f17-ca66a2350f51

2.5.) Numer ogłoszenia: 2025/BZP 00446184

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2025-09-29

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2025/BZP 00034568/06/P

2.10.) Identyfikator pozycji planu postępowań:

1.2.1 Poprawa cyberbezpieczeństwa w Gminie Jaraczewo

2.11.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.12.) Nazwa projektu lub programu:

Poprawa cyberbezpieczeństwa w Gminie Jaraczewo - Zadanie dofinansowane w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) 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: 2025/BZP 00326881

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: P-zp.271.01.07.2025

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

4.4.) Rodzaj zamówienia: Dostawy

4.5.1.) Krótki opis przedmiotu zamówienia

1. Zamówienie obejmować będzie wykonanie oprogramowania umożliwiającego świadczenie usługi „Audit as a Service” oraz świadczenie usługi „Audit as a Service” - stałego automatyzowanego audytu 24/7 wraz z monitoringiem infrastruktury w formie i zakresie usług cyberbezpieczeństwa, obsługi incydentów, kompletnych wdrożeń i konfiguracji sprzętu oraz niezbędnego oprogramowania, wraz ze stworzeniem oraz licencją dedykowanej platformy chmurowej w formuie SaaS zawierającej dodatkowo platformę szkoleniową. W zakres przedmiotu zamówienia wchodzi również licencja na ww. oprogramowanie stworzone w ramach wykonywania zamówienia na okres nie krótszy niż 5 lat.

2. Charakterystyka zamówienia obejmuje wykonanie i wdrożenie oprogramowania oraz zagwarantowanie względem Zamawiającego dostarczenia niezbędnego sprzętu i licencji oprogramowań będących w pełni zintegrowanych, skonfigurowanych i kompatybilnych ze stworzonym oprogramowaniem realizującym „przedmiot zamówienia” a uwzględniających możliwe wykorzystanie elementów posiadanej już infrastruktury.

3. Wyżej wymienione założenia wykonania przedmiotu zamówienia względem Wykonawcy powinny obejmować w ramach jego realizacji.:

- 1) stworzenie dedykowanego oprogramowania pozwalającego na dostęp do panelu web umożliwiającego 24/7 podgląd na interaktywną mapę infrastruktury, wyniki audytu, incydenty i status ich realizacji, status wdrożenia rekomendacji, alerty poszczególnych urządzeń, dokumentację, szczegółowe dane dla poszczególnych końcówek, raporty z możliwością eksportu danych;
- 2) audyt i zabezpieczenie wszystkich urządzeń, w tym: stacji roboczych (Windows, MacOS, Linux), serwerów (Windows, MacOS, Linux), domen internetowych, adresacji IP, pracowników i ich tożsamości, skrzynek pocztowych, drukarek, urządzeń sieciowych, zbiorów danych osobowych, serwerów plików, kopii zapasowych, chmur Microsoft i Google.
- 3) graficzną prezentację w formie punktacji stanu bezpieczeństwa poszczególnych elementów systemów i konfiguracji możliwą prezentacją widoków zbiorowych, grupowanych oraz szczegółowych;
- 4) audyt w trybie 24/7 zawierający minimum 300 kontrolek audytowych;
- 5) usługę reagowania na incydenty, w tym rozpoznanie incydentu, izolacja urządzeń i sieci, blokowanie autoryzacji, komunikacja z CERT i UODO;
- 6) weryfikację kopii zapasowych, przyjętego harmonogramu (np. GFS), dokumentacji Disaster Recovery, wspiera Business Continuity, RPO, RTO;
- 7) automatyzację i monitoring (SIEM i SOAR).
- 8) integrację z wdrożonym rozwiązaniem EDR/XDR/MDR, antywirusem, UTM, serwerem logów;
- 9) integrację z nowymi lub już wdrożonymi rozwiązaniami security;
- 10) zaawansowane urządzenie do skanowania podatności, sieci, konfiguracji;
- 11) dostęp do platformy e-learningowej z profilowanymi szkoleniami z obszaru cyberbezpieczeństwa wspomaganymi AI, zakończonych testem, bazy wiedzy, baza zagrożeń, które mogą dotyczyć konkretnej stacji roboczej i usług, z których korzysta użytkownik.

4. Zamawiający wymagać będzie od Wykonawcy dodatkowych usług wsparcia, które będą obowiązywać co najmniej do 31.05.2026 r.:

- 1) newsletter bezpieczeństwa, co najmniej raz na dwa miesiące ;
- 2) profilowane informacje o aktualnych trendach w atakach hakerskich, co najmniej raz na kwartał;
- 3) co najmniej 3 stacjonarne szkolenia z obszaru cyberbezpieczeństwa dla wszystkich pracowników Urzędu;
- 4) konsultacje z vCISO w kwestii podnoszenia bezpieczeństwa, wdrażania usług, tworzenia procedur, obsługi incydentów, generowanie raportów, szkolenie z mitygacji aktualnych zagrożeń;
- 5) comiesięczną weryfikację przez audytora wewnętrznego zakończoną raportem bezpieczeństwa zgodnym z Krajowymi Ramami Interoperacyjności (KRI);

- 6) stały monitoring widoczności w sieci publicznej z poziomu narzędzi dostępnych dla potencjalnego hakera, w tym baz, wycieków, wyszukiwarek, skanerów bezpieczeństwa;
- 7) konsultacje z audytorem wewnętrznym - min. 1 godzina miesięcznie w sesji zdalnej;
- 8) przekazywanie rekomendacji z pomocą przy ich wdrożeniu;
- 9) przegląd i aktualizację dokumentacji SZBI najpóźniej do 28 lutego 2026 r..

5. Ponadto w ramach wykonywania przedmiotu zamówienia Wykonawca dostarczy i skonfiguruje niezbędny sprzęt oraz licencje w terminie do 90 dni od podpisania umowy:

- 1) oprogramowanie do wykonywania kopii zapasowej i przestrzeń backup - zawiera licencje realizujące odmiejscową, odporną na ransomware kopię zapasową wraz z usługą monitoringu, disaster recovery i utrzymanie business continuity – 1 komplet
- 2) licencje na system EDR i XDR wraz z obsługą incydentów - zaawansowany antywirus i ochrona DNS wraz monitoringiem oraz obsługą incydentów na czas realizacji zamówienia - 40 licencji
- 3) licencje Mailbox Protection - zaawansowana ochrona poczty - m.in. filtr antyspamowy, anti-phishing, filtrowanie SPF, DKIM, sandbox, usługa wdrożenia, konfiguracji i reagowania na incydenty – 40 licencji
- 4) Przedłużenie licencji UTP dla posiadanego FortiGate 40F na czas trwania projektu– 1 szt.
- 5) Serwer w konfiguracji:
 - min. 16 slotów na dyski, min. 128GB RAM, Kontroler zdalnego dostępu, Zasilacze min. 2x700W, Windows Server 2022 Standard,
 - min. 2x 480GB SSD SATA 6Gb/s 512 2,5" dysk AG do intensywnego odczytu wymieniany bez wyłączania systemu w hybrydowym koszyku 3,5", 1 DWPD,
 - min. 2x 1,92TB SSD SATA 6Gb/s 512 2,5" dysk AG do intensywnego odczytu z możliwością wymiany bez wyłączania systemu, koszyk hybrydowy 3,5", 1 DWPD
 - min. 3x 4TB 7,2 tys. obr./min SATA 6Gb/s 512e 3,5" dysk twardy wymieniany bez wyłączania systemu 1 szt.
- 6) Serwer plików - konfiguracja min. dyski twarde 6TB 3.5" 8 szt., min. 16GB RAM – 1 szt.
- 7) FortiSwitch 148F lub sprzęt równoważny (tj. rozwiązanie równoważne musi posiadać min. 48 portów RJ45 Gigabit Ethernet, min. 4x SFP+, obsługę 10G, obsługę VLAN (min. 4000), Przepustowość routowania min. 176 Gbit/s , przepustowość min. 260 Mpps, możliwość montażu w szafie Rack 1U, pamięć DDR3- min. 512 MB, pamięć flash min. 64 MB, Certyfikaty FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2). : 2 szt.

8) Mobilny agregat prądowłórczy 50kVh – 1 szt.

9) Certyfikaty SSL - 1 kpl.

10) FortiToken lub urządzenie równoważne (tj. rozwiązanie równoważne musi służyć jako dodatkowa warstwa zabezpieczenia dostępu do sieci w formie „tokenu”- fizycznego urządzenia, podłączanego do portu USB, które umożliwia dwustopniową weryfikację. Rozwiązanie musi obsługiwać protokoły FIDO U2F oraz FIDO2 i musi być kompatybilne z systemami Windows/ Mac OS/ Linux)– 25 szt.

6. Zamówienie obejmuje udzielenie na minimum 24 miesięcy gwarancji na wszystkie dostarczone w ramach realizacji zamówienia urządzenia w formule „Next Business Day” dla dostarczonego sprzętu polegające na udzieleniu gwarancji na dostarczenie w 24H robocze, sprzętu zastępczego w pełni zintegrowanego, skonfigurowanego i kompatybilnego ze stworzonym oprogramowaniem umożliwiającym realizację „przedmiotu zamówienia”.

7. W przypadku gdyby w opisie przedmiotu zamówienia zostały wskazane nazwy producenta, nazwy własne, znaki towarowe, patenty lub pochodzenie materiałów służących do wykonania zamówienia - dopuszcza się możliwość zastosowania materiałów równoważnych. Oznacza to, że przewidziane przez Wykonawcę do zastosowania na etapie realizacji zamówienia urządzenia/rozwiązania/oprogramowania powinny spełniać co najmniej parametry określone w dokumentacji i nie powinny być gorsze od jej założeń. Zamawiający dopuszcza wszelkie rynkowe odpowiedniki o parametrach równych lub lepszych niż wskazane. Ciężar udowodnienia, że urządzenie/rozwiązanie/oprogramowanie jest równoważne w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy. W takim wypadku Wykonawca musi przedłożyć odpowiednie dokumenty opisujące parametry techniczne, wymagane prawem certyfikaty i inne dokumenty dopuszczające dane urządzenia/rozwiązania/oprogramowania do użytkowania, oraz pozwalające jednoznacznie stwierdzić, że są one rzeczywiście równoważne lub lepsze.

4.5.3.) Główny kod CPV: 48000000-8 - Pakiety oprogramowania i systemy informatyczne

4.5.4.) Dodatkowy kod CPV:

30233000-1 - Urządzenia do przechowywania i odczytu danych

31122000-7 - Jednostki prądowłórcze

32420000-3 - Urządzenia sieciowe

48219700-3 - Pakiety oprogramowania do serwera komunikacyjnego

48620000-0 - Systemy operacyjne

48710000-8 - Pakiety oprogramowania do kopii zapasowych i odzyskiwania

48732000-8 - Pakiety oprogramowania do zabezpieczania danych

48761000-0 - Pakiety oprogramowania antywirusowego

48820000-2 - Serwery

72263000-6 - Usługi wdrażania oprogramowania

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: 1

6.1.1.) Liczba otrzymanych ofert wariantowych: 0

6.1.2.) Liczba ofert dodatkowych: 0

6.1.3.) Liczba otrzymanych od MŚP: 1

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: 0

6.1.7.) Liczba ofert zawierających rażąco niską cenę lub koszt: 0

6.2.) Cena lub koszt oferty z najniższą ceną lub kosztem: 632900,00 PLN

6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 632900,00 PLN

6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 632900,00 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: Tak

7.2.) Wielkość przedsiębiorstwa wykonawcy: Mikro przedsiębiorca

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

7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia (dotyczy pełnomocnika, o którym mowa w art. 58 ust. 2 ustawy): Inveo Systems sp. z o.o.

Nazwy (firmy) pozostałych wykonawców wspólnie ubiegających się o udzielenie zamówienia: Nbit Jarosław Jenczmionka sp. z o.o.

7.3.2) Krajowy Numer Identyfikacyjny: 7812012994

7.3.3) Ulica: Łagowska

7.3.4) Miejscowość: Poznań

7.3.5) Kod pocztowy: 60-456

7.3.6.) Województwo: wielkopolskie

7.3.7.) Kraj: Polska

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

SEKCJA VIII UMOWA

8.1.) Data zawarcia umowy: 2025-09-10

8.2.) Wartość umowy/umowy ramowej: 632900,00 PLN

8.3.) Okres realizacji zamówienia albo umowy ramowej:
do 2026-05-31

8.4.) Zamawiający przewiduje następujące wymagania związane z realizacją zamówienia:

w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art. 95 ustawy

SEKCJA IX INFORMACJE DODATKOWE

Przedmiot zamówienia należy zrealizować w terminie od dnia podpisania umowy do dnia 31 maja 2026, przy czym:

- 1) dla pkt. 1., 2. i 3. i 5. rozdz. IV SWZ- termin wykonania zamówienia wynosi nie więcej niż 90 dni od dnia podpisania umowy;
- 2) Dla pkt dla pkt 4 i pkt 9 rozdz. IV SWZ– zamówienie należy wykonać do dnia 28 lutego 2026 r.