Załącznik nr 1 do zapytania ofertowego

nr IZP.271.26.2025

**OPZ – Opis przedmiotu zamówienia**

Zamawiający:

**Gmina Jabłonna Lacka**

adres: **ul. Targowa 4, 08-304 Jabłonna Lacka**

**NIP: 8212529494, REGON: 711582492**

**Zadanie pn.: „Usługi doradcze z zakresu cyberbezpieczeństwa oraz wykonywanie czynności techniczno- konfiguracyjno-organizacyjnych podnoszących poziom cyberbezpieczeństwa”**

*w ramach zadania pn.: „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Gminy Jabłonna Lacka przez wdrożenie SZBI, podniesienie świadomości pracowników oraz zakup sprzętu i usług zwiększających cyberbezpieczeństwo w ramach projektu „Cyberbezpieczny samorząd”*

1. Wykonawca zobowiązuje się zrealizować Przedmiot zamówienia w terminie od 1 stycznia 2026r. do 31 grudnia 2026r..
2. Wykonawca zobowiązuje się do wykonywania usług doradczych, informatycznych wzmacniających odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych zgodnie z ***„§3 punkt 2 podpunkt 3) obszar techniczny litera d) zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa - Regulaminu Konkursu Grantowego pn. “Cyberbezpieczny Samorząd” Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie na Rozwój Cyfrowy 2021-2027*”**, obejmujących niżej wymienione czynności na rzecz Urzędu Gminy Jabłonna Lacka:
   1. świadczenie usług doradczych w zakresie cyberbezpieczeństwa,
   2. świadczenie usług konfiguracyjnych posiadanej infrastruktury sieciowej, serwerowej oraz nowo zakupionego sprzętu – zapewniającej podniesiecie bezpieczeństwa danych (cyberbezpieczeństwa);
   3. świadczenie usług konfiguracyjnych w zakresie sprzętu komputerowego oraz oprogramowania, w których niezbędny będzie przyjazd do siedziby – Zamawiającego, zapewniającej podniesiecie bezpieczeństwa danych (cyberbezpieczeństwa),
   4. świadczenie tzw. Help Desku, tj. zdalnej pomocy w godzinach pracy Urzędu w celu rozwiązania problemów niewymagających przyjazdu do siedziby Zamawiającego, związanych z bezpieczeństwem danych – cyberbezpieczeństwem,
   5. usługa testowania bezpieczeństwa aplikacji, prowadzenie nadzoru nad bezpieczeństwem wykorzystywanego oprogramowania oraz znajomość obsługi wymienionych poniżej programów:
      1. Ewidencji ludności „SELWIN” z modułem rejestr wyborców „RWWIN” oraz Źródło,
      2. Systemu wspomagania budżetu „BESTIA” i „SJO BESTIA”,
      3. System Płatnik autorstwa Asseco,
      4. Programy autorstwa Tensoft,
      5. Legislator,
      6. Proton autorstwa Nefeni,
      7. Serwis www na platformie samorząd.gov.pl oraz BIP Urzędu na platformie ssdip.bip.gov.pl,
   6. usługa testowania bezpieczeństwa infrastruktury sieciowej, zapewnienie bezpieczeństwa sieci komputerowej i systemów – konfiguracja i zarządzanie systemami wykrywania zagrożeń sieciowych,
   7. opracowanie koncepcji oraz praktyczne wprowadzenie zabezpieczeń infrastruktury sieciowej / serwerowej / bazodanowej, w tym wykonywanie czynności ponoszących poziom cyberbezpieczeństwa określonych w SZBI,



* 1. usługa testowania bezpieczeństwa infrastruktury serwerowej, konfiguracja i ciągłe monitorowania oraz podnoszenie bezpieczeństwa infrastruktury serwerowej Urzędu Gminy, dokonywanie przeglądów, aktualizowanie oprogramowania zwiększającego poziom bezpieczeństwa,
  2. usługa testowania bezpieczeństwa infrastruktury sieciowej, monitorowanie oraz analiza stan techniczny sprzętu i oprogramowania,
  3. stosowanie / wnioskowanie o wdrożenie - środków technicznych mających na celu zabezpieczenie danych osobowych, zwiększających poziom bezpieczeństwa informacji,
  4. przygotowanie koncepcji oraz wdrożenie odpowiedniego systemu antywirusowa oraz jego centralne zarządzanie, monitorowanie i reakcja w przypadku wystąpienia zagrożenia,
  5. opracowanie koncepcji tworzenia kopii zapasowych baz danych oraz nadzór nad jej wykonywaniem,
  6. okresowa usługa testowania bezpieczeństwa - sprawdzanie kopii zapasowych pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
  7. zapewnienie bezpieczeństwa danych przetwarzanych w sieci komputerowej Urzędu Gminy przed niepowołanym dostępem z sieci zewnętrznej w tym monitorowanie logów UTM, analiza, działania prewencyjne,
  8. podniesienie poziomu cyberbezpieczeństwa przez konfigurowanie odpowiednich polityk na urządzeniach będących w posiadaniu Urzędu Gminy, tj. FortiGate 40F, FortiSwitch 148F, FortiAP 221E, w tym konfiguracja NAC.
  9. podniesienie poziomu cyberbezpieczeństwa przez optymalizacją struktur domenowych Active Directory w celu zapewnienia ich zgodności z nowoczesnymi standardami bezpieczeństwa,
  10. wprowadzenie odpowiedniej metodologii prowadzenie aktualizacji systemów w tym firmware – oprogramowania sprzętowego oraz wykonywania kopii ustawień konfiguracyjnych urządzeń kluczowych, w celu podniesienia bezpieczeństwa informacji,
  11. usługa testowania bezpieczeństwa aplikacji - konsultowanie zmian w oprogramowaniu oraz kontakty z autorami oprogramowania w zakresie polepszenia bezpieczeństwa danych,
  12. usługa testowania bezpieczeństwa serwisów internetowych - monitorowanie bezpieczeństwa strony internetowej Urzędu Gminy,
  13. usługa testowania bezpieczeństwa serwisów internetowych - monitorowanie bezpieczeństwa strony podmiotowej Biuletynu Informacji Publicznej,
  14. inne związane z poprawą cyberbezpieczeństwa oraz jakości pracy rozwiązań

teleinformatycznych.

1. Wykonawca w godzinach pracy Zamawiającego zapewni stały kontakt telefoniczny z osobami upoważnionymi do jego reprezentowania.
2. Wykonawca zobowiązuje się do przyjazdu do siedziby Zamawiającego **nie rzadziej niż raz** w tygodniu **w ustalony z Zamawiającym dzień**.
3. Strony ustalają przyjmowanie zgłoszeń przez Wykonawcę pod numerami telefonów lub pocztą elektroniczną na adres. Reakcja Wykonawcy do 2 godzin od zgłoszenia.

# SLA:

1. Przystąpienie do rozwiązywania zgłoszonych problemów od momentu zgłoszenia dla:
   1. incydentu bezpieczeństwa uniemożliwiającego pracę całego systemu nastąpi nie dłużej niż w czasie 4 godzin,
   2. incydentu bezpieczeństwa uniemożliwiającego korzystanie z poszczególnych stacji roboczych, lecz nie wykluczających pracy systemu na innych stanowiskach oraz dla innych mniej istotnych zdarzeń, nie powodujących wstrzymania systemu lub zatrzymania pracy Zamawiającego nastąpi nie dłużej niż w czasie 10 godzin,



* 1. incydentu bezpieczeństwa nie wpływających w sposób istotny na funkcjonowanie Systemu nastąpi nie dłużej niż w czasie 24 godzin,
  2. dla innych czynności nastąpi nie dłużej niż w czasie 2 dni roboczych.

# Gwarancja:

Zakres szczegółowo opisany w umowie.