

## Załącznik nr 5 do Zapytania ofertowego

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przegląd, aktualizacja, opracowanie i wdrożenie SZBI wraz z dokumentacją i szkoleniami zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2023, uwzględniające wdrożenie zarządzania ciągłością działania w oparciu o obowiązujące wymagania norm ISO 22301 i aktualne wymagania prawne dla urzędu gminy Gojnik i jednostki podległej Gminny Ośrodek Pomocy Społecznej

## ZAMAWIAJĄCY

Urząd Gminy Gnojnik 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 Gnojnik*, którego celem jest poprawa jakości bezpieczeństwa usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji w kontekście zwiększenia poziomu cyberbezpieczeństwa.

Urząd Gminy Gnojnik zatrudnia 46 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 Gminny Ośrodek Pomocy Społecznej w Gnojniku zatrudnia 10 Regulamin organizacyjny oraz schemat znajdują na stronie internetowej urzędu pod wskazanym adresem internetowym:

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

## PRZEDMIOT ZAMÓWIENIA

### Usługa

Przegląd, aktualizacja, opracowanie i wdrożenie SZBI wraz z dokumentacją i szkoleniami zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2023, uwzględniające wdrożenie zarządzania ciągłością działania w oparciu o obowiązujące wymagania norm ISO/IEC 22301 i wymagania prawne dla urzędu gminy Gojnik i jednostki podległej Gminny Ośrodek Pomocy Społecznej

CPV: 79417000-0 Usługi doradcze w zakresie bezpieczeństwa

CPV: 72225000-8 Usługi w zakresie oceny i analizy gwarancji jakości systemu

CPV: 71620000-0 Usługi analizy

CPV: 79212000-3 Usługi audytu

## TERMIN REALIZACJI USŁUGI

Od podpisania umowy i nie dłużej 12.12.2025 r. Maksymalny czas realizacji usługi do 12 mcy.

Realizacja usługi zostanie potwierdzona protokołem końcowym odbioru.

## SZCZEGÓŁOWY ZAKRES ZAMÓWIENIA

Wykonawca w ramach przedmiotu zamówienia będzie świadczyć usługi konsultacyjne, doradcze, prace analityczne, szkoleniowe oraz przeprowadzi audyt wstępny i powdrożeniowy celem przeglądu, aktualizacji opracowania i wdrożenia SZBI wraz z dokumentacją i szkoleniami zgodnie z aktualnymi wymaganiami normy PN-EN ISO/IEC 27001:2023, uwzględniając wdrożenie zarządzania ciągłością działania w oparciu o obowiązujące wymagania norm PN-EN ISO 22301 i wymagania prawne. Wykonawca kompleksowo przeprowadzi Zamawiającego przez proces systemowego podejścia do zarządzania bezpieczeństwem i ciągłością działania, poczynając od ustalenia kontekstu organizacji i celów bezpieczeństwa, po przygotowanie wymaganych normą PN-EN ISO/IEC 27001:2023 procesów, dokumentów a następnie ich wdrożenie oraz ciągłości działania bezpieczeństwa informacji i cyberbezpieczeństwa zgodnie z PN-EN ISO 22301:2019.

Etapy realizacji prac i warunki świadczenia usług:

1. Audyt wstępny (przegląd) stanu środowiska Zamawiającego pod kątem zgodności z obowiązującymi regulacjami prawnymi przed ustanowieniem i wdrożeniem SZBI oraz ciągłości działania uwzględniając świadczone usługi przy wykorzystaniu IT oraz przedstawienie raportu z audytu wstępnego wraz z oceną.
2. Aktualizacja, opracowanie i wdrożenie „Polityki bezpieczeństwa informacji w Urzędzie Gminy w Gnojniku oraz jednostce podległej GOPS w tym analiza kontekstu wewnętrznego i zewnętrznego, ustalenie celów i mierników bezpieczeństwa zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2023 oraz norm ISO 27005:2022 i ISO 31000:2018;
3. Opracowanie materiałów informacyjnych i szkoleniowych dotyczących Polityki bezpieczeństwa informacji wprowadzającej SZBI, skierowanych do kierownictwa, pracowników Urzędu Gminy i jednostki organizacyjnej w Gnojniku wraz ze szkoleniem w tym zakresie.
4. Wypracowanie metodyki zarządzania aktywami informacyjnymi w Urzędzie Gminy i jednostce organizacyjnej w Gnojniku, uwzględniającej cykl życia informacji, przypisanie właścicieli aktywów do realizowanych celów i zadań oraz działalności urzędu.
5. Wykonawca opracuje mechanizm pozwalający na przeprowadzenie identyfikacji i klasyfikacji aktywów. Prace dot. identyfikacji aktywów docelowo zostaną zawarte w rejestrze aktywów informacyjnych urzędu. Wykonawca będzie wspierał Zamawiającego poprzez konsultacje w zakresie sposobu realizacji prac. Wykonawca przeprowadzi instruktaż dla kluczowych osób zaangażowanych w identyfikację aktywów w urzędzie w zakresie sposobu realizacji opracowanej metodyki i jej zapisów.
6. Opracowanie i wdrożenie metodyki zarządzania ryzykiem bezpieczeństwa informacji i cyberbezpieczeństwa w oparciu o ISO 27005:2022 i ISO 31000:2018. Opracowanie autorskiej metody zarządzania ryzykiem, zdefiniowanie ról i zakresu odpowiedzialności. Przeprowadzenie

procesu zarządzania ryzykiem i wdrożenie go w urzędzie. Integracja procesu z innymi systemami (np. w zakresie ochrony danych osobowych, kontroli zarządczej), jeśli Zamawiający tak uzna po konsultacjach z Wykonawcą. Przeprowadzenie warsztatów z osobami zaangażowanymi bezpośrednio w proces zarządzania ryzykiem.

7. Wdrożenie, aktualizacja i opracowanie dokumentacji SZBI wymaganej normy PN-EN ISO/IEC 27001:2023, tj. opracowanie i wdrożenie polityk dziedzinowych, procedur, instrukcji zgodnie z załącznikiem A do normy i samej normy. Przeprowadzenie konsultacji dla całej organizacji. Wykonawca na podstawie wyników uzyskanych w trakcie realizacji audytu wstępnego (badania) o którym mowa w pkt. 1, identyfikacji i klasyfikacji aktywów informacyjnych, identyfikacji świadczonych usług przy wykorzystaniu IT oraz wyników szacowania ryzyka, przedstawi mapę dokumentów SZBI stanowiącą szczegółowy wykaz dokumentów z określeniem ich wzajemnych powiązań.
8. Na podstawie zatwierdzonej przez Zamawiającego propozycji mapy dokumentów SZBI, Wykonawca opracuje wszystkie opisane w koncepcji dokumenty i procedury oraz inne zapisy uwzględniając współpracę z osobami odpowiedzialnymi za realizację procesów i kierownikami komórek organizacyjnych. Dokumenty te muszą być zgodne ze wszystkimi wymaganiami prawnymi.
9. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego na każdym etapie realizacji zamówienia.
10. Przeprowadzenie analizy wpływu na biznes określającej krytyczne aktywa urzędu i jednostki, dopuszczalne czasy niedostępności świadczonych usług przy wykorzystaniu IT, czas odtworzenia po katastrofie. Opracowanie i wdrożenie planów ciągłości dla tych usług lub ich komponentów zgodnie z normą PN-EN ISO 22301:2019
11. Zamawiający wymaga opracowania dokumentacji w liczbie zapewniającej kompletny zakres realizowanych zadań IT w urzędzie.
12. Audyt powdrożeniowy. Przeprowadzenie audytu powdrożeniowego na zgodność PN-EN ISO/IEC 27001:2023, który dokona oceny funkcjonowania SZBI i przedstawi jego wyniki w raporcie z audytu.
13. Usługa ma być wykonana w oparciu o procesy wskazane w normie ISO/IEC TS 27022 Technologia informacyjna – Wytyczne dotyczące procesów systemu zarządzania bezpieczeństwem informacji, uwzględniając procesy dodatkowe, w przypadku wdrożenia kontroli z załącznika A normy PN-EN ISO/IEC 27001:2023 oraz samej normy.
14. Każdy proces ma być przypisany w zakresie odpowiedzialności zgodnie z opracowaną macierzą RACI.

#### UWAGA

Zamawiający zastrzega sobie weryfikację przeglądu, aktualizacji, opracowania i wdrożenia SZBI zgodnie z wymaganiami określonymi w przedmiocie zamówienia i zasadami konkursu dla projektu grantowego pn. *Wzmocnienie odporności cyfrowej w Gminie Gnojnik*, wyłącznie w zakresie odpowiedzialności wykonawcy wynikającej z realizacji usługi w celu zapewnienia zgodności realizacji projektu grantowego.

## OGÓLNY HARMONOGRAM REALIZACJI ZAMÓWIENIA

1. Etap I – Audyt wstępny (badanie/przegląd) przed ustanowieniem i wdrożeniem SZBI – do 20 dni od podpisania umowy.
2. Etap II – Aktualizacja, opracowanie i wdrożenie Polityki bezpieczeństwa informacji w urzędzie – do 40 dni od podpisania umowy.
3. Etap III – Aktualizacja, opracowanie i wdrożenie metodyki zarządzania aktywami informacyjnymi urzędu – do 30 dni od zakończenia etapu II.
4. Etap IV – Aktualizacja, opracowanie i wdrożenie metodyki zarządzania ryzykiem – do 40 dni od zakończenia etapu III.
5. Etap V – Aktualizacja, opracowanie i wdrożenie dokumentacji SZBI zgodnej z ISO 27001 – prace powinny zostać rozpoczęte po realizacji etapu I, jednakże powinny być zrealizowane nie dłużej niż 70 dni od zakończenia etapu IV.
6. Etap VI – Identyfikacja i opisanie świadczonych usług przy wykorzystaniu IT w urzędzie. Wypracowanie podejścia do zarządzania tymi usługami oraz opracowanie rejestru. Prace powinny rozpocząć się po zrealizowaniu etapu IV, a realizacja ich powinna zakończyć się w ciągu 70 dni.
7. Etap VII – Opracowanie i wdrożenie planów ciągłości działania dla usług IT. Przeprowadzenie analizy wpływu na biznes – prace powinny rozpocząć się po zrealizowaniu etapu V i VI, a realizacja ich powinna zakończyć się w ciągu 75 dni.
8. Etap VIII – Audyt powdrożeniowy – prace powinny rozpocząć się po zrealizowaniu etapu VII, a realizacja ich powinna zakończyć się w ciągu 20 dni.

## ORGANIZACJA REALIZACJI OPISU PRZEDMIOTU ZAMÓWIENIA

1. Wykonawca zapewni kierownika usługi, który będzie posiadał pełną wiedzę o realizowanej usłudze oraz będzie odpowiedzialny za komunikację w projekcie i podpisywanie raportów częściowych z etapów realizacji prac, przedstawianie harmonogramów oraz ewentualnych zmian.
2. Zamawiający zapewni zespół wdrażający w urzędzie.
3. Wykonawca przygotowuje harmonogram prac do akceptacji Zamawiającego.
4. W przypadku nieobecności kluczowego pracownika w trakcie trwania szkolenia/konsultacji, Wykonawca zapewni indywidualne wsparcie dla nieobecnych w innym dogodnym terminie. Zapewnienie wsparcia w danym zakresie/konsultacji może odbyć się ponownie jeden raz.
5. W ramach każdego etapu Wykonawca przeprowadzi przynajmniej jedno spotkanie inicjujące, na którym poinformuje w szczególności o harmonogramie pracy, sposobie realizacji, celach, produktach częściowych, kamieniach milowych.
6. W ramach etapów II-VII Wykonawca powinien przewidzieć konsultacje u Zamawiającego w liczbie nie mniejszej niż 60 godzin online i min. 20 godzin w siedzibie. W sytuacji wprowadzenia pracy zdalnej u Zamawiającego lub z innych ważnych przyczyn, Zamawiający dopuszcza by konsultacje i spotkania realizowane były on-line za pomocą komunikatora internetowego, który zapewni Wykonawca. Dla Zamawiającego obsługa komunikatora musi być nieodpłatna.

7. Zamawiający wymaga informowania w formie pisemnej o przebiegu realizacji prac z uwzględnieniem każdego etapu.
8. Każdy etap prac uznaje się za zakończony po przyjęciu przez obie strony protokołu z zakończenia prac danego etapu. Przyjęcie pracy jest tożsame z wypłatą częściowego wynagrodzenia.
9. 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.
10. 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.
11. Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty niniejszego zamówienia.
12. Wykonawca w ramach 12 miesięcznej gwarancji, liczonej od dnia zakończenia ostatniego etapu, zobowiązany będzie do poprawy błędów w przekazanej dokumentacji niezależnie od jej formy wytworzenia, w terminie nie dłuższym niż 15 dni od daty zgłoszenia błędu przez Zamawiającego.

## DOKUMENTY WYTWORZONE W RAMACH REALIZACJI PROJEKTU

Dokumenty operacyjne osobno dla Urzędu i jednostki organizacyjnej, co najmniej:

1. Raport z badania przed ustanowieniem i wdrożeniem SZBI.
2. Polityka bezpieczeństwa informacji.
3. Polityki tematyczne do PBI.
4. Procedury, instrukcje, procesy, formularze, schematy.
5. Materiały informacyjne dot. PBI.
6. Ankieta skierowana do właścicieli aktywów.
7. Metodyka identyfikacji aktywów wraz z dokumentami operacyjnymi.
8. Rejestr aktywów zgodnie z ISO 27005.
9. Metodyka zarządzania ryzykiem wraz z dokumentami operacyjnymi.
10. Rejestr ryzyk IT.
11. Mapa dokumentów SZBI.
12. Pełna dokumentacja SZBI.
13. Rejestr świadczonych usług przy wykorzystaniu IT.
14. Ankieta BIA.
15. Plany ciągłości działania dla usług IT (około 6 dokumentów).
16. Raport z audytu powdrożeniowego.

Dokumenty zarządcze co najmniej:

1. Harmonogram realizacji etapów I-VIII.
2. Raport wstępny.
3. Dokumentacja SZBI.
4. Listy obecności ze szkoleń i materiały szkoleniowe.
5. Raport końcowy.