

Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

I. Zamówienie obejmuje Przeprowadzenie audytów zgodności z wymaganiami KRI

II. Liczba jednostek objętych zamówieniem 3 jednostki (Urząd oraz 2 podległe JST):

- Urząd Gminy Bodzechów z/s w Ostrowcu Św.
- Gminny Ośrodek Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św.
- Gminnego Centrum Oświaty w Bodzechowie

III. Ilość stanowisk komputerowych:

- Urząd Gminy Bodzechów z/s w Ostrowcu Św. – 50
- Gminny Ośrodek Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św. – 12
- Gminnego Centrum Oświaty w Bodzechowie – 5

IV. Opis przedmiotu zamówienia:

1. Wykonawca jest zobowiązany do przeprowadzenia audytów KRI w poszczególnych latach realizacji projektu grantowego „Cyberbezpieczny Samorząd” tj. w roku:

- **2024** łącznie 3 audyty KRI w trzech jednostkach tj. w Urzędzie Gminy Bodzechów z/s w Ostrowcu Św., Gminnym Ośrodku Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św. i Gminnym Centrum Oświaty w Bodzechowie, zostaną przeprowadzone od dnia zawarcia umowy nie później niż do **12.12.2024r.**

- **2025** łącznie 3 audyty KRI w trzech jednostkach tj. w Urzędzie Gminy Bodzechów z/s w Ostrowcu Św., Gminnym Ośrodku Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św. i Gminnym Centrum Oświaty w Bodzechowie, zostaną przeprowadzone od dnia **01.07.2025** do dnia **31.10.2025**

- **2026** łącznie 3 audyty KRI w trzech jednostkach tj. w Urzędzie Gminy Bodzechów z/s w Ostrowcu Św., Gminnym Ośrodku Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św. i Gminnym Centrum Oświaty w Bodzechowie, zostaną przeprowadzone od dnia **02.03.2026** do dnia **30.04.2026**

2. Wykonawca musi wykazać, że w ciągu ostatnich **3 lat** przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – to w tym krótszym okresie – wykonał **należycie co najmniej** cztery usługi, z których każda obejmowała swoim zakresem przeprowadzenie audytu systemu bezpieczeństwa informacji obejmującego zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001 lub równoważnej (Wymagamy uzupełnienia **Załącznika nr 4 – Wykaz usług**).

3. Zakres audytów KRI (systemu bezpieczeństwa informacji) każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 pkt 14 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773) oraz zgodność z wymaganiami normy PN ISO/IEC 27001 dla Zamawiającego.

4. Zakres przeprowadzanych audytów na podstawie przepisów:

- 1) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
- 2) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
- 3) Ustawa o krajowym systemie cyberbezpieczeństwa.
- 4) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679
- 5) Normy ISO 27001.

5. Dla każdej jednostki po wykonanym audycie wymagamy oddzielnego raportu. Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań Rozporządzenia KRI. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzejelementowej skali: 1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone, 2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego” jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników), 3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

6. Forma przeprowadzenia audytów – stacjonarna w miejscu audytowanej jednostki.

7. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.

8. Audyty KRI dla Zamawiającego muszą zostać przeprowadzone przez:

1) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. 2018 poz. 1999) lub audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001.

2) audytor przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 4 audyty systemu bezpieczeństwa informacji obejmującego zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001 lub równoważnej (Wymagamy uzupełnienia **Załącznika nr 5 – Wykaz osób**).

9. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego.

10. Wykonawca po wykonaniu audytów KRI w 2026 roku jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych). Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta” dla Zamawiającego na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.

11. Jednostki samorządu terytorialnego oraz jego jednostki podległe, które biorą udział w projekcie „Cyberbezpieczny Samorząd” są zobowiązane do przesłania do NASK raportu z audytu KRI oraz wypełnionej ankiety dojrzałości cyberbezpieczeństwa. Niezwłocznie po ich przekazaniu przez Wykonawcę dokumenty te zostaną przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z tej dokumentacji przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze także powyżej wskazany cel przeprowadzenia zamówienia i jego przeznaczenie.

12. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.

13. Zobowiązuje się Wykonawcę do wprowadzania niezbędnych zmian w dokumentacji i aktualizacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w terminie do dnia 31.05.2026 r.