

Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

I. Zamówienie obejmuje Przeprowadzenie wdrożenia, przeglądu, aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i Polityki Bezpieczeństwa Informacji (PBI) spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji i w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania wg ISO 22301. Całość zamówienia musi być zrealizowana zgodnie z warunkami i wytycznymi konkursu grantowego „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC).

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

- 1) Urząd Gminy Bodzechów z/s w Ostrowcu Św. (UG)
- 2) Gminny Ośrodek Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św. (GOPS)
- 3) Gminne Centrum Oświaty w Bodzechowie (GCO)

III. Ilość stanowisk komputerowych:

- 1) Urząd Gminy Bodzechów z/s w Ostrowcu Św. – **50**
- 2) Gminny Ośrodek Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św. – **12**
- 3) Gminne Centrum Oświaty w Bodzechowie – **5**

IV. Opis przedmiotu zamówienia:

1. Wykonawca jest zobowiązany do przeprowadzenia wdrożenia, przeglądu, aktualizacji SZBI i PBI w 2025 roku realizacji projektu grantowego „Cyberbezpieczny Samorząd” tj.: łącznie **3** wdrożenia, przegląd, aktualizacja SZBI i PBI 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 **31.10.2025r.**

„SZBI” - należy przez to rozumieć System Zarządzania Bezpieczeństwem Informacji

„PBI” - należy przez to rozumieć Politykę Bezpieczeństwa Informacji

Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb UG, GOPS i GCO dokumentację SZBI z wymaganiami powołanych wyżej norm.

Celem wdrożenia jest zapewnienie wysokiego poziomu bezpieczeństwa informacji w jednostce i spełnienie wymagań:

- 1) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
 - 2) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
 - 3) Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (tzw. Dyrektywa NIS 2).
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 opracowania i wdrożenia dokumentacji SZBI obejmującego zgodność z kryteriami zawartymi w § 19 ust. 2 rozporządzenia KRI oraz zgodność z wymaganiami normy PN-ISO/IEC 27001 lub równoważnej w tym minimum jednej w urzędach administracji samorządowej (Wymagamy uzupełnienia **Załącznika nr 4 – Wykaz usług** a także dołączenia dokumentów potwierdzających wykonanie usługi np. referencji).

Ponadto Wykonawca skieruje do wykonania zamówienia co najmniej 2 osoby spełniające warunki opisane poniżej. Wdrożenie, przegląd, aktualizacja SZBI i PBI dla Zamawiającego muszą zostać przeprowadzone przez:

- 1) osobę skierowaną do wykonania zamówienia posiadającą odpowiednie kwalifikacje zawodowe niezbędne do wykonania usługi mającą przynajmniej jeden aktualny z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu
- 2) osobę skierowaną do wykonania zamówienia, która w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli ten okres jest krótszy – to w tym krótszym okresie – przeprowadziła przynajmniej 4 opracowania i wdrożenia dokumentacji SZBI obejmującego zgodność z kryteriami zawartymi w § 19 ust. 2 rozporządzenia KRI oraz zgodność z wymaganiami normy PN-

ISO/IEC 27001 lub równoważnej w tym minimum jednej w urzędach administracji samorządowej (Wymagamy uzupełnienia **Załącznika nr 5 – Wykaz osób**).

3. Zakres prac obejmuje w szczególności:

- 1) Sprawdzenie i zrozumienie środowisk UG, GOPS oraz GCO, obejmujący aktualną strukturę organizacyjną i realizowane procesy oraz wymagania prawne ich funkcjonowania.
- 2) Przegląd aktualnej dokumentacji bezpieczeństwa informacji (jeśli istnieje), w tym polityk, procedur, instrukcji, regulaminów, wytycznych.
- 3) Inwentaryzację i analizę aktywów - zasobów informacyjnych oraz środków służących do gromadzenia i przetwarzania informacji.
- 4) Przeprowadzenie przy udziale przedstawicieli Zamawiającego i udokumentowanie analizy ryzyka, w tym opracowanie i wdrożenie metodyk.
- 5) Wskazanie obszarów wymagających dostosowania i/lub doskonalenia adekwatnie do przeprowadzonej analizy ryzyka oraz wymagane do wdrożenia zabezpieczenia.
- 6) Opracowanie i przekazanie zamawiającemu na podstawie protokołu odbioru kompletnej dokumentacji SZBI (wszystkich wymaganych przez powołane normy polityk, planów, procedur, instrukcji, metodologii zarządzania ryzykiem itd.)

Opracowane polityki, procedury itd. muszą realnie odnosić się do procesów w UG, GOPS oraz GCO.

Zamawiający oczekuje, że opracowane dokumenty będą napisane zwięźle, językiem zrozumiałym dla osób nie posiadających wysokiego przygotowania z zakresu bezpieczeństwa informacji.

Jednocześnie Zamawiający zastrzega, że wszelkie błędy w przygotowanej dokumentacji świadczące o tym, że dokumentacja została przeniesiona z innej organizacji będą podstawą do odrzucenia dokumentów do poprawki, bez ich dalszej analizy ze strony Zamawiającego.

Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę nowego SZBI, w tym do rodzaju dokumentów, ich liczby, nazewnictwa, zakresu

4. Opracowana i wdrożona dokumentacja SZBI musi być zgodna z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:

- 1) rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie krajowych ram interoperacyjności;

- 2) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1);
 - 3) 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)
 - 4) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
 - 5) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z późn. zm.);
 - 6) normami ISO, m.in: PN-ISO/IEC 27001:2023, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-EN ISO 22301;
 - 7) Nowe SZBI zostaną przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie pisemnej.
5. Forma przeprowadzenia wdrożenia, przeglądu, aktualizacji SZBI i PBI – stacjonarna w miejscu siedziby Zamawiającego.
6. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz z raportami z przeprowadzonych audytów KRI w 2024 roku 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.
7. Jednostki samorządu terytorialnego oraz jej 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.

8. 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.**