



IOZK.271.3.2026

**Gmina Pionki  
ul. Zwycięstwa 6a  
26-670 Pionki**

**„Szczegółowy opis przedmiotu zamówienia – Wykonanie audytu oraz dokumentacji SZBI”  
realizowane w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),  
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu  
cyberbezpieczeństwa, Konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny  
Samorząd”**

**I .USŁUGA PRZEPROWADZENIA AUDYTU WSTĘPNEGO – KRI/UOKSC ORAZ SZBI DLA  
URZĘDU GMINY PIONKI, A TAKŻE DWÓCH JEDNOSTEK ORGANIZACYJNYCH:**

Zamawiający wymaga realizacji usługi dla łącznie trzech jednostek, tj:

- Urząd Gminy Pionki;
- Gminny Ośrodek Pomocy Społecznej w Pionkach;
- Gminny Zarząd Oświaty i Sportu w Pionkach;

Audyt wstępny ma zostać przeprowadzony w oparciu o normę ISO/IEC 27001, ocenę spełniania wymagań określonych w Krajowych Ramach Interoperacyjności (KRI), Ustawie o Krajowym Systemie Cyberbezpieczeństwa (KSC), oraz innych obowiązujących przepisach prawa regulujących zarządzanie bezpieczeństwem informacji. Zamawiający wymaga, aby audyt został przeprowadzony w w/w jednostkach.

Audyt bezpieczeństwa informacji obejmuje wszystkie obszary funkcjonowania Zamawiającego w tym co najmniej:

**1. Audyt organizacyjny:**

- 1) weryfikacja regulacji w obszarze zarządzania bezpieczeństwem informacji;
- 2) odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;





- 3) dokumentacja, w tym z zakresu ochrony danych osobowych;
- 4) analiza ryzyka;
- 5) inwentaryzacja aktywów;
- 6) plan postępowania z ryzykiem;
- 7) przeprowadzenie wywiadów z wybranymi pracownikami.

## 2. Audyt fizyczny i środowiskowy

- 1) weryfikacja zabezpieczeń wejścia/wyjścia;
- 2) weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;
- 3) weryfikacja bezpieczeństwa okablowania strukturalnego;

## 3. Audyt teleinformatyczny

- 1) weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi;
- 2) przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania i ciągłości działania;
- 3) weryfikacja ochrony przed oprogramowaniem szkodliwym;
- 4) weryfikacja procedur zarządzania kopiami zapasowymi;
- 5) weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
- 6) weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
- 7) weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);
- 8) Analiza i ocena mechanizmów zarządzania aktualizacją.

W wyniku przeprowadzonego audytu Wykonawca sporządzi i prześle zamawiającemu Raport, który będzie zawierał co najmniej ocenę stanu, rekomendacje i wyniki audytu.

## **II. USŁUGA OPRACOWANIA DOKUMENTACJI SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA URZĘDU GMINY PIONKI, A TAKŻE DWÓCH JEDNOSTEK ORGANIZACYJNYCH:**

Zamawiający wymaga realizacji usługi dla łącznie trzech jednostek, tj:

1. Przegląd i aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla jednostki:

- Urząd Gminy Pionki:



2. Opracowanie oraz wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla jednostek:

- Gminny Ośrodek Pomocy Społecznej w Pionkach;
- Gminny Zarząd Oświaty i Sportu w Pionkach

Zamawiający wymaga wykonania usługi zgodnie z wymaganiami bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych oraz aktualnie obowiązującymi normami PN-EN ISO 27001 oraz PN-EN ISO 22301, w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd” realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

Zamawiający wymaga, aby dokumentacja w swoim zakresie obejmowała przynajmniej:

**Projektowanie systemu zarządzania bezpieczeństwem informacji poprzez następujące procedury i zagadnienia:**

1. Opracowanie procedury identyfikacji wymagań dla Systemu Zarządzania Bezpieczeństwem Informacji
  - a) Identyfikacja zainteresowanych stron
  - b) Inwentaryzacja wymagań prawnych, branżowych, umownych i innych wymagań związanych z bezpieczeństwem informacji
  - c) Określenie ról i osób odpowiedzialnych za spełnienie w/w wymagań
2. Opracowanie Polityki Bezpieczeństwa Informacji
  - a) Określenie Zakresu Systemu Zarządzania Bezpieczeństwem Informacji
  - b) Opis celów zarządzania bezpieczeństwem informacji
  - c) Przypisanie odpowiedzialności i ról w zakresie utrzymywania SZBI
3. Przygotowanie Metodyki Szacowania i Postępowania z Ryzykiem
  - a) Opis metodyki
  - b) Określenie sposobu wyliczenia ryzyka
  - c) Opis metod akceptacji poszczególnych wartości ryzyka
  - d) Stworzenie wzoru tabeli szacowania ryzyka, tabeli postępowania z ryzykiem, tabele zawierają przykładowe aktywa, zagrożenia i podatności
  - e) Wzór raportu z dokonanego szacowania ryzyka
  - f) przeprowadzenie przez Wykonawcę analizy ryzyka bezpieczeństwa informacji
4. Opracowanie Deklaracji stosowania, która zawiera opis zastosowania poszczególnych form zabezpieczeń



5. Opracowanie Planu postępowania z ryzykiem, zawierający opis działania z poszczególnym ryzykiem wraz z szczegółowymi informacjami na temat działań, które mają zostać podjęte
6. Przygotowanie procedury audytu wewnętrznego
  - a) Opis opracowywania planów audytu
  - b) Opis metod przeprowadzania audytów oraz opracowywania raportów
  - c) Dodatkowo dołączony wzór rocznego programu audytu wewnętrznego
7. Przygotowanie wzoru protokołu z przeglądu SZBI dokonywanego przez kierownictwo
8. Przygotowanie procedury działań naprawczych i działań korygujących w ramach wykrytych niezgodności
9. Przygotowanie Procedur Operacyjnych dla zarządzania systemami informatycznymi zawierające:
  - a) Polityki haseł
  - b) Polityki rozwoju systemów informatycznych, zawierające wzór wykazu systemów
  - c) Procedury dot. kopii zapasowych, wraz z wzorcem zasad ich tworzenia i przechowywania
  - d) Procedury dot. środowiska testowego i eksploatacji systemów wraz z dokumentowaniem zmian wraz z przygotowanymi wzorcami dokumentacji dotyczącej infrastruktury teleinformatycznej
  - e) Procedury niszczenia danych i wycofania systemów z eksploatacji
  - f) Procedury zabezpieczenia systemów
  - g) Procedury dot. posługiwania się nośnikami wymiennymi
  - h) Procedury dotyczące pracy w sieci Internet
  - i) Procedury dotyczące korzystania z poczty elektronicznej (regulamin)
  - j) Procedury dotyczące serwisu i przeglądu systemów informatycznych
  - k) Procedury dotyczące monitoringu infrastruktury i raportowania funkcjonowania środowiska teleinformatycznego