Znak sprawy: SG.271.2.10.2024

Załącznik nr 2 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest wsparcie eksperckie w zakresie przeglądu, aktualizacji i opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnej z normą ISO/IEC 27001:2023.

Wykonawca musi zrealizować usługę polegającą na przeprowadzeniu audytu cyberbezpieczeństwa w Urzędzie Gminy Zębowice w ramach projektu „Cyberbezpieczny samorząd" w Urzędzie Gminy Zębowice zgodnie z zakresem oraz formularzem stanowiącym załącznik do Regulaminu Konkursu Grantowego „Cyberbezpieczny samorząd" zakończonego raportem oraz opracowanie i wdrożenie pełnej kompletnej dokumentacji SZBI w oparciu o KRI/KSC i normę ISO27001. Wykonanie i przekazanie Raportu z Audytu (opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów, analiza złożonego zał. nr 6 konkursu grantowego).

Audyt bezpieczeństwa informacji obejmuje wszystkie obszary funkcjonowania Zamawiającego:

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;
4) weryfikacja systemów chłodzenia i systemów alarmowych.

3. Audyt teleinformatyczny

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