Załącznik nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Informacje ogólne. Cel zamówienia.

1. Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych w JST, poprzez opracowanie strategicznych i szczegółowych uregulowań w zakresie bezpieczeństwa informacji przez opracowanie Polityki Bezpieczeństwa Informacji.
2. Przedmiot zamówienia będzie realizowany w ramach projektu konkursu grantowego pn. „Cyberbezpieczny Samorząd" realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Priorytet II: Zaawansowane usługi cyfrowe (dalej: konkurs „Cyberbezpieczny Samorząd").
3. Opracowana w wyniku niniejszego postępowania Polityka Bezpieczeństwa Informacji będzie aktualizować stan bezpieczeństwa informacji, w tym zwłaszcza w kontekście zadań realizowanych w ramach konkursu „Cyberbezpieczny Samorząd" i zgodnie z dokumentami opracowanymi w ramach ww. konkursu, w tym zwłaszcza „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", stanowiącej Załącznik nr 6 do Regulaminu konkursu Cyberbezpieczny Samorząd.

II. Szczegółowy opis przedmiotu zamówienia.

1. Przedmiotem zamówienia jest usługa obejmująca weryfikację zastanego stanu rzeczy w aspekcie bezpieczeństwa informacji przechowywanej i przetwarzanej w JST oraz opracowanie Polityki Bezpieczeństwa Informacji.
2. Polityka Bezpieczeństwa Informacji musi być sporządzona zgodnie z normą PN-ISO/IEC 27001 i musi obejmować/zawierać/uwzględniać:
    1. Polityki bezpieczeństwa
    2. Niezbędnych materiałów do samodzielnej oceny ryzyka przez JST
    3. Planu Ciągłości Działania
    4. Polityki Zarządzania Danymi
    5. Polityki Zarządzania Incydentami
    6. Polityki Zarządzania Dostępami
    7. Polityki Zarządzania Podatnościami
    8. Polityki Zarządzania Szyfrowaniem Danych

9. Polityki Zarządzania Zasobami Oprogramowania
10. Klasyfikację kontekstu: zewnętrznego i wewnętrznego.

3. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej przez Wykonawcę dokumentacji. Wykonawca zobowiązany jest do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.
4. Szczegółowy harmonogram realizacji zamówienia będzie ustalany z Zamawiającym po podpisaniu umowy. Zamawiający zadba o dostępność dokumentacji potrzebnej do przygotowania Polityki Bezpieczeństwa Informacji.
5. Na zakończenie realizacji zamówienia Wykonawca przekaże Zamawiającemu opracowaną Politykę Bezpieczeństwa Informacji w wersji papierowej oraz elektronicznej.