*Załącznik nr 4 b do SWZ*

**OPIS PRZEDMIOTU ZAMÓWIENIA   
do części 2   
 Szkolenia z cyberbezpieczeństwa**

w postępowaniu o udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji o wartości zamówienia mniejszej niż kwoty określone w obwieszczeniu Prezesa Urzędu Zamówień Publicznych, ogłoszonym na podstawie art. 3 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz.U. z 2022 r. poz. 1710 ze zm.)

realizowanego w ramach projektu

**„Cyfrowa Gmina”**

**Zamawiający**: Gmina Skoczów, ul. Rynek 1, 43-430 Skoczów

## INFORMACJE O ZAMAWIAJĄCYM

**Gmina Skoczów**

**Rynek 1, 43-430 Skoczów**

## PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest przeprowadzenie szkoleń dla 80 urzędników w zakresie cyberbezpieczeństwa.
2. Szkolenia będą się odbywały w dni robocze, w godzinach 8:00 – 15:00, w co najmniej 3 grupach szkoleniowych
3. Forma szkolenia: w trybie on-line za pomocą udostępnionej przez wykonawcę platformie.
4. Szkolenie dla jednej grupy szkoleniowej będzie trwało min. 5 godzin.
5. Szkolenia muszą obejmować następujące zagadnienia:
   1. Co to jest cyberprzestępczość
   2. Opis funkcjonowania zorganizowanych grup cyberprzestępczych
   3. Czy naprawdę nam zagrażają
   4. Czy jestem atrakcyjnym „klientem” dla cyberprzestępcy
   5. Jakie zyski może mieć cyberprzestępca atakując moje dane
   6. Straty wynikające z udanego ataku na firmę
   7. Rodzaje ataków skierowane w pracowników biurowych
   8. Jak cyberprzestępca dołącza nasz komputer do sieci Botnet
   9. Jak się przed tym bronić
   10. Spam jako niegroźny sposób na groźne ataki
   11. Handel adresami e-mail
   12. Kampanie phishingowe jako metoda okradania naszych kont bankowych
   13. Opłacalność ataków DoS/DDoS wymierzonych w naszą instytucję
   14. Groźne ataki 0-day - czy istnieje sposób obrony przed nimi
   15. Nieopłacona FV jako sposób przemycenia wirusa do naszego systemu
   16. Skąd cyberprzestępca zna moje hasło
   17. Skanowanie kart płatniczych - gdzie i kiedy ktoś zeskanował moja kartę
   18. Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych
   19. Przekazywanie haseł dostępowych współpracownikom
   20. Fizyczne bezpieczeństwo miejsca pracy
   21. Znaleziony pendrive na parkingu jako pozwolenie na atak dla cyberprzestępcy
6. Szkolenia prowadzone będą w języku polskim na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac z dołączonym zakresem merytorycznym, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 7 dni przed rozpoczęciem szkolenia.
7. W ramach szkoleń, wykonawca zapewni: nieodpłatne materiały szkoleniowe w formie elektronicznej, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz zaświadczenia o ukończeniu szkolenia dla wszystkich uczestników.
8. Szkolenia muszą być prowadzone przez kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

## TERMIN WYKONANIA ZAMÓWIENIA

Termin realizacji zamówienia – **do 30 dni** od daty podpisania umowy.