Załącznik nr 1 do SWZ

Nr postępowania: WIR.271.5.2025

**OPIS PRZEDMIOTU ZAMÓWIENIA – Zadanie 2 obszar kompetencyjny**

**Pozycja 2. Szkolenia dla pracowników z zakresu cyberbezpieczeństwa**

Opis szczegółowy usługi szkoleń z zakresu bezpieczeństwa informacji, ochrony danych osobowych i cyberbezpieczeństwa

1. Przedmiot zamówienia:
   1. Usługa na szkolenia stacjonarnego i w formie online
   2. Szkolenia dedykowane dla pracowników biurowych (nietechnicznych) pracujących z komputerami i przetwarzających różnego rodzaju informacje o różnym poziomie poufności.
   3. Świadczenie usługi szkolenia musi obejmować:
      1. przeprowadzenie dwóch szkoleń stacjonarnych (po 3h oraz dwóch szkoleń online (po 3h) – zakończonych testami (w tym zaraportowanie wyników testów – raport ma zostać przedstawiony dzień po ukończeniu wszystkich szkoleń)
      2. przygotowanie materiałów informacyjnych (przypominających) do rozdysponowania pracownikom po ukończeniu szkoleń.
      3. Szkolenie musi zostać przeprowadzone przez trenera, która ma doświadczenie w szkoleniach z cyberbezpieczeństwa i ochrony danych osobowych dla jednostek publicznych – do oferty należy dołączyć dwie pisemne potwierdzenia przeprowadzenia szkoleń w jednostkach publicznych.
2. Szkolenie musi posiadać oddzielne lekcje dla co najmniej następujących zagadnień:
   1. Czym jest bezpieczeństwo informacji, ochrona danych osobowych i cyberbezpieczeństwa?
   2. Aspekty prawne związane z bezpieczeństwem informacji, ochroną danych osobowych i cyberbezpieczeństwem.
   3. Czym jest phishing?
   4. Zasady korzystania z Internetu.
   5. Zasady korzystania z portali społecznościowych.
   6. Zasady korzystania z poczty elektronicznej i zagrożenia z tym związane.
   7. Zasady korzystania z bezpiecznych haseł.
   8. Zagrożenia i sposoby zabezpieczania sprzętu mobilnego.
   9. Metody pozyskiwania informacji (socjotechnika).
   10. Bezpieczeństwo w zakresie płatności elektronicznych.
   11. Bezpieczeństwo fizyczne w zakresie zabezpieczania pomieszczeń, dokumentacji, sprzętu IT.
   12. Czym jest ransomware i jak wygląda w praktyce?
   13. Techniki stosowane przez cyberprzestępców.
   14. Praca zdalna - jak zrealizować ją bezpiecznie?
   15. Vishing… co to jest? .
   16. Fake news i dezinformacja.
   17. Incydenty bezpieczeństwa – prawidłowa reakcja
   18. Test z imiennym certyfikatem ukończenia kursu.
3. Forma szkolenia :
   1. Szkolenie musi posiadać atrakcyjną formę przekazu materiału, zachęcającą osoby uczące się do aktywnego odbywania szkolenia. Atrakcyjna forma to m. in. Grafika oparta na przykładach, ćwiczeniach, testach sprawdzających wiedzę.
   2. W celu zwiększenia praktycznej przydatności szkolenia musi ono zostać opracowane tak, aby zajęcia kładły większy nacisk na umiejętności praktyczne użytkowników komputerów (np. wykrywanie sytuacji zagrożenia w trakcie korzystania z serwisów społecznościowych, właściwe postępowanie w razie incydentu, wykrywanie wiadomości phishingowych) niż samą teorię bezpieczeństwa IT
   3. Cały materiał szkolenia musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne.
   4. Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001.