*Załącznik nr 2*

ZAMAWIAJĄCY:

**Gmina Chełmno**

**ul. Dworcowa 5**

**86-200 Chełmno**

RSO.ASI.271.2.2024.JZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Przedmiotem zamówienia jest przeprowadzenie szkoleń ramach projektu grantowego „Cyberbezpieczny Samorząd”:**
   1. **Szkolenie** **z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy w Chełmnie**
   2. **Szkolenie** **z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji dla pracowników Urzędu Gminy w Chełmnie**

**Zakres szkoleń powinien obejmować między innymi następujące zagadnienia:**

* + 1. Co nam zagraża? Co dzieje się obecnie w Polsce i na świecie? Przykłady ataków.
    2. Kradzieże i wyłudzenia informacji – przykłady z życia urzędów
    3. Kultura ochrony informacji, dojrzałość organizacji.
    4. Straty wynikające z udanego ataku na firmę – omówienie i przykłady.
    5. Bezpieczeństwo w organizacji. Obowiązki jednostek publicznych wynikające z aktualnego stanu prawnego w obszarze bezpieczeństwa informacji - KRI – Krajowe Ramy Interoperacyjności.
    6. Składowe systemu zarządzania bezpieczeństwem informacji.
    7. Socjotechniki, przykłady zastosowania.
    8. Metody codziennej ochrony informacji - praca z danymi osobowymi w urzędzie i poza nim, fizyczne bezpieczeństwo miejsca pracy, dobre praktyki.
    9. Rodzaje ataków:
       - poczta elektroniczna;
       - ataki BPC, BEC, APT;
       - komunikatory;
       - programy biurowe (MS Office);
       - ataki pasożytnicze;
       - ataki ransomware i jak z nimi sobie radzić.
    10. Cyberbezpieczeństwo w pracy zdalnej – omówienie, dobre praktyki/wskazówki.
    11. Szyfrowanie dokumentów w ramach dostępnych funkcji w pakiecie Office.
    12. Szyfrowanie dowolnego pliku programem zewnętrznym.
    13. Bezpieczeństwo urządzeń mobilnych.
    14. Fake news - jak je identyfikować i walka z fałszywymi wiadomościami.
    15. OSINT (biały wywiad) przykłady i zastosowanie w Urzędzie.
    16. Sesja pytań i odpowiedzi.

W przypadku szkoleń dla wybranych przedstawicieli kadr JST, tematyka podanych zagadnień powinna także uwzględniać obowiązki ciążące na kadrze kierowniczej oraz zawierać dodatkowe tematy:

* + 1. Rola i obowiązki kadry kierowniczej w zakresie cyberbezpieczeństwa wynikające z aktów prawnych i wdrożonych polityk.
    2. Organy i instytucje zwalczające zagrożenia w cyberprzestrzeni.
    3. Charakterystyka stopni alarmowych CRP – zagrożenia i obowiązki.

1. **Wymagania dotyczące organizacji szkoleń:**
   1. **Szkolenie z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy w Chełmnie**
      1. szkolenie ma odbyć się w trybie stacjonarnym:
      * dla pracowników Urzędu Gminy w Chełmnie na terenie Urzędu Gminy (sala sesyjna), ul. Dworcowa 5, 86-200 Chełmno do 10.12.2024 r.
      1. Wykonawca przeprowadzi szkolenie w dwóch grupach, przy czym szkolenia tych grup nie mogą trwać jednocześnie, aby nie powodować utrudnień w ciągłości pracy danej Jednostki;
      2. w szkoleniu udział będzie brało 20 pracowników (podzielonych na 2 grupy);
      3. szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami);
      4. szkolenie powinno odbyć się w dni robocze, w godzinach pracy Urzędu Zamawiającego;
      5. szkolenie musi być prowadzone w języku polskim;
   2. **Szkolenie z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji dla pracowników Urzędu Gminy w Chełmnie** 
      1. szkolenie odbędzie się w trybie stacjonarnym:
      * dla pracowników Urzędu Gminy w Chełmnie na terenie Urzędu Gminy (sala sesyjna), ul. Dworcowa 5, 86-200 Chełmno do 10.12.2024 r.
      1. Wykonawca przeprowadzi szkolenie w jednej grupie;
      2. w szkoleniu udział będzie brało 4 pracowników;
      3. szkolenie dla jednej grupy powinno trwać minimum 3 godziny zegarowe (łącznie z przerwami);
      4. szkolenie powinno odbyć się w dni robocze, w godzinach pracy Urzędu Zamawiającego;
      5. szkolenie musi być prowadzone w języku polskim;
2. **Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z wymogami określonymi poniżej:**
   1. Wykonawca zapewni:
      1. osobę prowadzącą szkolenie, która posiada wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia;
      2. wydanie uczestnikom szkolenia po jego zakończeniu zaświadczenia/certyfikatu o ukończeniu szkolenia;
      3. prowadzenie dokumentacji szkolenia, na którą składają się:
         * lista obecności uczestników szkolenia,
         * lista uczestników szkolenia, którym wydano zaświadczenia/certyfikaty o ukończeniu szkolenia;
      4. oznakowanie w odpowiedni sposób wszelkiej dokumentacji szkolenia, zgodnie z zasadami oznakowania projektu grantowego pn.: „Cyberbezpieczny Samorząd”;
   2. Wykonawca zobowiązany jest po przeprowadzeniu szkolenia do przekazania dokumentacji szkolenia zamawiającemu w wersji papierowej;
   3. Wykonawca pokrywa wszelkie koszty związane z wykonaniem przedmiotu zamówienia, w tym koszty swojego ewentualnego zakwaterowania, dojazdu, wyżywienia, przygotowania materiałów szkoleniowych (druku itp.).