Opis Przedmiotu Zamówienia

1 Szkolenie z zakresu cyberbezpieczeństwa

Liczba uczestników	Około 30 osób
Liczba godzin szkoleniowych	4
Liczba dni szkoleniowych	1
Forma szkolenia	Stacjonarne w siedzibie Zamawiającego
Infrastruktura dostarczana przez Zamawiającego	Sala szkoleniowa, rzutnik, projektor,
Infrastruktura dostarczana przez Wykonawcę	Materiały szkoleniowe, komputery, o ile są wymagane specyfiką szkolenia.
Cel szkolenia	Szkolenie obejmuje zagadnienia związane z cyberbezpieczeństwem w Urzędzie Gminy Przechlewo
Wymagania wobec wykonawcy	-Przeprowadzenie min 1 szkolenie z cyberbezpieczeństwa – na dowód wykonawca przedstawi referencje - uprawnienia : wykształcenie wyższe, - ukończone szkolenie audytora wiodącego systemu zarzadzania bezpieczeństwem informacji wg normy PN-EN ISO/IEC 27001- na dowód wykonawca przedstawi certyfikat lub inny certyfikat potwierdzający posiadania wiedzy z zakresu cyberbezpieczeństwa (wykaz certyfikatów Ministra Cyfryzacji uprawnionych do przeprowadzenia audytów)
Minimalny zakres szkolenia	Zakres szkolenia obejmie następujące zagadnienia: 1. Wstęp o Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne o Ryzyko i zarządzanie ryzykiem - co to jest ryzyko, podstawowe pojęcia i zasady zarządzania ryzykiem o Polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola o Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować o Normy i standardy bezpieczeństwa - powszechnie stosowane rozwiązania, norma ISO27001 2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji) o Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców o Sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty o Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego o Reakcja - jak prawidłowo reagować na ataki socjotechniczne o Jak i skąd atakujący zbierają dane na twój temat o Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacji w sieci

	3. Atak „na komputery” - demonstracje wraz z objaśnieniem metod ochrony o Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących o Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC) o Ataki przez pocztę e-mail (fałszywe e-maile) o Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony o Ataki przez komunikatory (Skype, Facebook) o Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.) o Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam 4. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów o Polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych o Bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty, „czyste biurko” o Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop) o Problem aktualnego oprogramowania i kopii zapasowych o Bezpieczna praca z pakietem biurowym Microsoft Office o Bezpieczna praca z programem pocztowym o Bezpieczna praca z przeglądarką internetową o Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty) 5. Aspekty prawne o Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji o Nieautoryzowane użycie systemów komputerowych o Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego o Dane osobowe i dane wrażliwe