Ramowy zakres szkolenia urzędników w zakresie cyberbezpieczeństwa
dla
Urzędu Miasta Janowiec Wielkopolski

1. **Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika**
2. **Polityka bezpieczeństwa w organizacji. Definicja**
3. **Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem w urzędzie**
4. **Integralność, poufność, dostępność. Definicje**
5. **Istotne obszary bezpieczeństwa z punktu widzenia pracowników urzędu z uwzględnieniem:**
   a. **bezpieczeństwa fizycznego** (miejsca pracy)
      - dokumenty
      - urządzenia
      - czyste biurko
      - czysty ekran
   b. **bezpieczeństwa organizacyjnego** (personalnego), w tym:
      - postępowanie w celu zapewnienia bezpieczeństwa informacji, w szczególności w ramach telepracy i pracy zdalnej, omówienie zasad bezpieczeństwa informacji oraz najlepszych praktyk zabezpieczających
      - zasady bezpieczeństwa podczas wideokonferencji
      - bezpieczne korzystanie z Internetu, ze szczególnym uwzględnieniem serwisów społecznościowych
      - prywatność w sieci czyli: trackery, ciastka (cookies), tryb incognito
      - rozpoznawania fałszywych informacji
      - fake news - identyfikacja i walka z fałszywymi wiadomościami
   c. **bezpieczeństwa informacyjnego** (informacje, dane, zasoby)
      - bezpieczne korzystanie z sieci Wi-Fi
      - zdalny dostęp do firmowych zasobów
      - bezpieczeństwo danych w chmurze
6. **Prawidłowe korzystanie z komputera**
   a. Zasady aktualizacji programów, aplikacji, oprogramowania antywirusowego
   b. w jaki sposób zabezpieczyć własne dane
      - szyfrowanie dokumentów i poczty elektronicznej.
      - archiwizacja
   c. Polityka haseł, zarządzanie dostępem i tożsamością.
      - jak tworzyć silne hasło (propozycje)?
      - przechowywania hasła,
      - odzyskiwanie hasła i dostępu do systemu operacyjnego
   d. bezpieczeństwo zakupów oraz płatności w Internecie
7. **Rodzaje ataków. Przyczyny, źródła, cel i mechanizmy ataków.**
   a. ataki socjotechniczne,

b. ataki komputerowe,
c. ataki przez sieci bezprzewodowe,
d. ataki przez pocztę e-mail (fałszywe e-maile),
e. ataki przez strony WWW,
f. ataki przez telefon,
g. Czym są, definicje: phishing, spoofing, phishing, pharming, sniffing, ransomeware, malware, spam

8. **Czym jest socjotechnika i jak się przed nią bronić?**
   a. metody ochrony przed atakami komputerowymi i socjotechnicznymi,
   b. stosowanie technik socjotechnicznych w informatyce
   c. zdefiniowanie pojęcia przy użyciu przykładów, z którymi pracownicy mogą spotkać się w codziennej pracy,
   d. przedstawienie sposobów manipulacji mających na celu uzyskanie określonych korzyści, zwrócenie uwagi, że nawet najmniejsza ilość informacji może przyczynić się do penetracji organizacji,
   e. przeciwdziałanie atakom socjotechnicznym (np. podszywanie się pod służby ochrony, współpracownika lub firmę współpracującą, interesanta, pracownika biurowego na urlopie itp.;
   f. profilowanie, zbieranie informacji o podmiocie ataku i wybieranie najlepszego czasu na atak),
   g. pakiet biurowy i niebezpieczne dokumenty (m.in. bezpieczna konfiguracja pakietu, złośliwe makra, kradzież danych logowania i inne potencjalne ataki).
9. **Przykłady incydentów bezpieczeństwa informacji. Największe wycieki danych z ostatnich lat . Omówienie przykładów.**