ATFIDE

# Oferta Szkolenia

# pt;

# CYBERZAGROŻENIA

# W KONTEKŚCIE USTAWY O KRAJOWYM SYSTEMIE

# CYBERBEZPIECZEŃSTWA Z UWZGLĘDNIENIEM ROZPORZĄDZENIA KRI

## Szkolenie Zgodne z wymogami projektu Cyfrowa Gmina

- ✓ **Co muszą wiedzieć pracownicy w procesie wystąpienia naruszeń, zgłaszania incydentów oraz zarządzania ryzykiem.**

**Podstawa prawna:**

- *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r. poz. 526).*
- *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.*
- *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).*

**Celem szkolenia jest podniesienie umiejętności i wiedzy w zakresie przestrzegania zasad cyberbezpieczeństwa w związku ze wzrostem liczby cyberataków.**

**Szkolenie adresowane jest do wszystkich pracowników jednostki którzy przetwarzają informacje i dane podlegające prawnej ochronie.**

**Program Szkolenia;**

1. **Podstawowe pojęcia i uwagi wprowadzające**
   - cyberprzestrzeń
   - cyberbezpieczeństwo
   - incydenty i ich rodzaje
2. **Rodzaje i specyfika incydentów**
   - oszustwa komputerowe
   - drażliwe lub nielegalne treści

ATFIDE Sp. z o.o.
38-400 Krosno, ul. Tysiąclecia 14 pok. 14B
REGON: 382099880, NIP: 6842651623
Numer KRS: 0000763708

Kontakt: +48 692 125 822
+48 793 916 434
biuro@atfide.pl
www.atfide.pl

- złośliwe oprogramowania
- próby włamań
- gromadzenie informacji
- włamania
- dostępność zasobów
- atak na bezpieczeństwo informacji/socjotechnika
- inne jeśli mogą wystąpić w danej jednostce

**3. Zespoły Reagowania na incydenty**

- CSIRT MON
- CSIRT GOV
- CSIRT NASK

**4. Reakcje na incydenty i sposób ich zgłaszania**

5. **Zagrożenia bezpieczeństwa informacji i danych osobowych**

• utrata poufności informacji (wyciek i kradzież informacji)
• niebezpieczne oprogramowanie
• metody wyłudzania informacji, sposoby kradzieży danych
• zagrożenia przy użytkowaniu nośników zewnętrznych
• techniki włamań do komputerów pracowników
• ryzyko przetwarzania danych przy świadczeniu usług drogą elektroniczną
• ryzyko korzystania z sieci Internet
• korzystanie ze służbowej poczty elektronicznej, ryzyko przekazywania informacji poza jednostkę
• zabezpieczenie dokumentacji papierowej(tradycyjnej).

**Koszt szkolenia: do uzgodnienia**