Oferta

na przeprowadzenie szkolenia zamkniętego pt.:

OCHRONA i BEZPIECZEŃSTWO INFORMACJI

w jednostkach sektora publicznego

w świetle obowiązujących przepisów prawa

stosownie do §20 ust.2 pkt. 6 rozporządzenia KRI

- **co muszą wiedzieć pracownicy aby właściwie zabezpieczać informacje**

Szanowni Państwo,

Odpowiednia świadomość i wiedza pracowników oraz właściwy nadzór ze strony Kadry Kierowniczej pozwoli nie tylko uniknąć nieprawidłowości podczas ewentualnych postępowań kontrolnych właściwych organów administracji publicznej, ale również zapewnić właściwe standardy ochrony przetwarzanych informacji.

Przypominamy, że spoczywa na Państwu obowiązek **zapewnienia szkolenia wszystkim pracownikom jednostki zaangażowanym w proces przetwarzania informacji** stosownie do przepisów Rozporządzenia 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).*

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

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

PLAN SZKOLENIA:

<u>OCHRONA I BEZPIECZEŃSTWO INFORMACJI</u> *W ZAKRESIE:*

1. Zagrożenia bezpieczeństwa informacji;

a) utrata poufności informacji (wyciek i kradzież informacji)

b) niebezpieczne oprogramowanie

c) metody wyłudzania informacji, sposoby kradzieży danych

d) zagrożenia przy użytkowaniu nośników zewnętrznych

e) techniki włamań do komputerów pracowników

f) ryzyko przetwarzania danych przy świadczeniu usług drogą elektroniczną

g) ryzyko korzystania z sieci Internet

h) korzystanie ze służbowej poczty elektronicznej, ryzyko przekazywania informacji poza jednostkę

i) zabezpieczenie dokumentacji papierowej (tradycyjnej)

2. Praktyczne aspekty ochrony informacji

a) bezpieczeństwo - jako element prawnej ochrony informacji

b) podstawowe zadania i obowiązki Administratora danych

c) zasady stosowania odpowiednich do zagrożeń i kategorii danych objętych ochroną, środków zabezpieczeń zapewniających rzeczywiste bezpieczeństwo przetwarzania informacji

d) praktyczne aspekty i mechanizmy zabezpieczania informacji w tym danych osobowych/rola i zadania Administratora Systemu Informatycznego

e) zasady dostępu i odpowiedzialność osób upoważnionych do przetwarzania informacji

f) dokumentacja bezpieczeństwa informacji – ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwa Informacji /charakterystyka ogólna

g) uprawnienia kontrolne NIK, UW,PIP

3. Skutki naruszenia zasad bezpieczeństwa informacji /odpowiedzialność prawna;

Koszt przeprowadzenia szkolenia: *do uzgodnienia*