Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

**SZKOLENIE ON LINE**
**17 maja 2021 r.**

# Bezpieczna praca zdalna w administracji publicznej

## WAŻNE INFORMACJE O SZKOLENIU:

Praca zdalna stała się faktem i koniecznością. Także w administracji publicznej. Szczególnie poza murami urzędu należy dbać o skuteczną ochronę informacji. Przede wszystkim, należy zadbać o zwiększenie świadomości wśród pracowników oraz kadry zarządzającej dotyczące ochrony informacji (nie tylko danych osobowych) oraz rzeczywistych zagrożeń, a szczególnie cyberzagrożeń. W dobie szybkiej cyfryzacji usług oraz powszechnej pracy zdalnej, każdy dyrektor, kierownik i pracownicy powinni wiedzieć jak zagwarantować bezpieczeństwo informacji oraz jakie wymogi prawa muszą być spełnione, a także jakie sankcje grożą za ich złamanie.

- Czy wymagania KRI nadal są aktualne?
- Kiedy ostatnio przeprowadzany był audyt bezpieczeństwa w Twojej jednostce?
- Czy instytucje publiczne oraz pracownicy są celem ataków hackerskich?
- Czy wiesz jaki jest koszt wycieku lub kradzieży danych?
- Czy Twój rejestr incydentów/naruszeń ma jakieś wpisy?
- Jakie zadania i obowiązki czekają po wycieku danych?
- Czy znasz przykłady wycieku/kradzieży danych z innych podmiotów publicznych?
- Jak pracownicy zadbali o bezpieczeństwo stanowiska pracy w domu?
- A może pracownik dostał jakiś podejrzany e mail?
- Czy kliknął w link lub załącznik?
- Czy pracownicy wiedzą jak odróżnić fałszywe e-maile?
- Czy można wiarygodnie sprawdzić skuteczność cyberzabezpieczeń Twojej instytucji zanim dojdzie do prawdziwego ataku?

Proponujemy Państwu udział w szkoleniu, które pomoże poznać odpowiedzi na powyższe pytania, a także aktualne zagrożenia i skuteczne sposoby ochrony danych.

## CELE I KORZYŚCI:

- Omówienie zagadnień związanych z ochroną informacji w jednostkach publicznych, szczególnie podczas wykonywania pracy zdalnej.
- Przypomnienie prawnych aspektów bezpieczeństwa informacji.
- Wiele przykładów „z życia” dotyczących bezpieczeństwa informacji i cyberzagrożeń w jednostkach publicznych.
- Przykłady ataków socjotechnicznych na instytucje publiczne i zasad ochrony przed takimi atakami.
- Omówienie przydatnych narzędzi technicznych oraz organizacyjnych w zapewnieniu skutecznej ochrony informacji w codziennej pracy urzędnika.

## PROGRAM:

1. **Podstawy bezpieczeństwa informacji w urzędzie:**
   - Prawne aspekty bezpieczeństwa informacji czyli poza RODO tez istnieje życie.
   - Cyberbezpieczeństwo w urzędzie – przykłady.
   - Kradzieże, wycieki danych i inne zagrożenia w urzędzie.
   - Praca zdalna czyli urzędnik poza urzędem: zasoby, zagrożenia, podatności, zabezpieczenia
   - Jak przygotować bezpieczne stanowisko pracy w domu?
   - Jak bezpiecznie przewieźć dokumentacje i komputery z urzędu do domu?
   - Jak zachować poufność przesyłanych dokumentów np. poprzez e-mail?
2. **Ataki hackerskie / socjotechniczne:**
   - Przykłady ataków socjotechnicznych: spoofing /phishing.
   - Podejrzane e-maile w codziennej pracy urzędnika.
   - Czy pendrive od znajomego może być niebezpieczny?
   - Jak przetestować nasz urząd zanim dojdzie do ataku hackerskiego
3. **Hasło powinno być bezpieczne:**
   - Czy Twoje hasło do systemów informatycznych jest bezpieczne?
   - Jak stworzyć silne hasła i łatwo je zapamiętać?
   - Jak bezpiecznie chronić hasła, gdy mamy ich 199?
   - A jeśli samo hasło to za mało? Co to jest „2FA/MFA”?

## ADRESACI:

- Pracownicy jednostek administracji publicznej, szczególnie: kadr, finansów, zamówień publicznych i sekretariatów,
- Kadra zarządzająca jednostek administracji publicznej,
- Informatycy,

którzy chcą poznać i zrozumieć podstawy tematyki bezpieczeństwa informacji i cyberbezpieczeństwa w jednostkach administracji publicznej zgodnie z aktualnym stanem prawnym i zmieniającymi się zagrożeniami.

## PROWADZĄCY:

Specjalista w dziedzinie bezpieczeństwa informacji. Certyfikowany trener ECDL EPP e Urzędnik, egzaminator ECDL oraz kierownik projektów ICT (Fn-TSPM). Certyfikowany specjalista IT Security - CISS (Certified IT Security Specialist). Członek Polskiego Towarzystwa Informatycznego. Ma za sobą również kilkuletnie doświadczenie wykładowcy wyższej uczelni. Poprzednio kierownik Wydziału Informatyki w dużej jednostce administracji samorządowej. Był odpowiedzialny za kluczowe projekty informatyczne realizowane w urzędzie oraz skuteczne wdrażanie Polityki Bezpieczeństwa Informacji. Prowadzi szkolenia oraz konsultacje w firmach i administracji.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

# INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

## Bezpieczna prac zdalna w administracji publicznej

Szkolenie będziemy realizowali **w formie webinarium on line**.

**17 maja 2021 r.** **Szkolenie w godzinach 9:30-14:00**

**Cena: 299 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

| | |
|---|---|
| **CENA zawiera:** | udział w profesjonalnym szkoleniu on-line,<br>materiały szkoleniowe w wersji elektronicznej,<br>certyfikat ukończenia szkolenia,<br>możliwość konsultacji z trenerem. |
| **DANE DO KONTAKTU:** | Fundacja Rozwoju Demokracji Lokalnej Centrum Mazowsze<br>ul. Żurawia 43, 00-680 Warszawa<br>tel. (42) 307 32 65 fax: (42) 288 12 86<br>**szkolenia@frdl.org.pl** |

## DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

**Nazwa i adres nabywcy (dane do faktury)**

**Nazwa i adres odbiorcy**

**NIP** **Telefon**

1. **Imię i nazwisko uczestnika,**
   stanowisko,
   E-MAIL i TEL. DO KONTAKTU
2. **Imię i nazwisko uczestnika,**
   stanowisko,
   E-MAIL i TEL. DO KONTAKTU

**Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe)** TAK ☐ NIE ☐

**Proszę o certyfikat w formie:** Papierowej ☐
Elektronicznej ☐ e mail……

**Proszę o przesłanie faktury na adres mailowy: ……**

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora **www.frdl.mazowsze.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

**Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.mazowsze.pl lub mailem na adres szkolenia@frdl.org.pl do 12 maja 2021 r.**

UWAGA Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

**Podpis osoby upoważnionej** _____