Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

STACJONARNIE W KRAKOWIE
27 marca 2026 r.

CYBERBEZPIECZEŃSTWO W ADMINISTRACJI SAMORZĄDOWEJ - PRAKTYCZNE STRATEGIE OCHRONY DANYCH I PRZECIWDZIAŁANIA ATAKOM

WAŻNE INFORMACJE:

W dobie narastającej cyberprzestępczości, sektor administracji samorządowej stał się celem co piątego ataku hakerskiego. Ponieważ, aż 78% incydentów wynika z błędów ludzkich, kluczem do ochrony instytucji nie są wyłącznie systemy, ale przede wszystkim świadomi pracownicy. Nasze intensywne szkolenie wypełnia lukę między teorią a praktyką, dostarczając urzędnikom konkretnych narzędzi do walki z zagrożeniami. Podczas warsztatów uczestnicy opanują zasady higieny cyfrowej, które skutecznie chronią dane urzędowe, finanse oraz wizerunek urzędu przed zaawansowanymi metodami ataków.

CELE I KORZYŚCI:

- **Eliminacja błędów ludzkich:** Uczestnicy zdobędą umiejętność rozpoznawania i neutralizowania prób ataków, co drastycznie obniża ryzyko zainfekowania infrastruktury urzędu.
- **Biegłość w technologiach ochronnych:** Program gwarantuje praktyczne opanowanie narzędzi takich jak menedżery haseł, uwierzytelnianie wieloskładnikowe (MFA) oraz bezpieczne sieci VPN i systemy IDS/IPS.
- **Zarządzanie bezpieczeństwem danych:** Kadra nauczy się profesjonalnych metod szyfrowania informacji, bezpiecznego udostępniania dokumentów w chmurze oraz tworzenia niezawodnych kopii zapasowych.
- **Ochrona prywatności i mienia:** Szkolenie dostarcza wiedzy, jak chronić nie tylko dane służbowe, ale również prywatne oszczędności i tożsamość cyfrową pracowników w codziennej pracy i życiu osobistym.
- **Gotowy pakiet narzędziowy:** Każdy uczestnik otrzyma kompletny zestaw materiałów elektronicznych oraz zweryfikowaną bazę źródeł wiedzy, umożliwiającą natychmiastowe wdrożenie bezpiecznych nawyków w strukturach urzędu.

PROGRAM:

1. Zabezpieczenie sieci:
   - Zapory ogniowe (firewalle).
   - Wirtualne sieci prywatne (VPN).
   - Systemy wykrywania i zapobiegania włamaniom (IDS/IPS).
2. Ochrona urządzeń i systemów:
   - Antywirusy.
   - Zarządzanie aktualizacją oprogramowania.
   - Zarządzanie aplikacjami i ich uprawnieniami.
3. Zarządzanie hasłami oraz bezpieczne logowanie:
   - Tworzenie silnych haseł.
   - Używanie uwierzytelniania wieloskładnikowego (MFA).
   - Korzystanie z managerów haseł.
4. Zarządzanie prywatnością w internecie:
   - Kontrola prywatności na stronach internetowych.
   - Używanie pseudonimów.
5. Rozpoznawanie i unikanie zagrożeń:
   - Metody ataków.
   - Rodzaje ataków - rozpoznawanie zagrożeń.
   - Bezpieczne korzystanie i przesyłanie załączników.
   - Bezpieczne korzystanie z publicznych sieci Wi-Fi.
6. Zarządzanie danymi:

- Szyfrowanie danych w ruchu i w spoczynku (np. na urządzeniach, w chmurze).
- Bezpieczne i regularne tworzenie kopii zapasowych.
- Bezpieczne korzystanie z chmury.
- Udostępnianie dokumentów.
- Bezpieczne usuwanie danych.

7. Dobre nawyki cyfrowe:
   - Stosowanie zasad higieny cyfrowej w codziennej pracy.
   - Przykłady ataków sieciowych.
   - Case studies.
   - Rady praktyczne w życiu codziennym i pracy zawodowej.
   - Ważne aplikacje i usługi podnoszące bezpieczeństwo.

ADRESACI:

Kadra zarządzająca jst (w tym najwyższe kierownictwo podmiotu): prezydenci, burmistrzowie, wójtowie, starostowie, sekretarze, dyrektorzy, kierownicy. Pracownicy działów IT. Inspektorzy ochrony danych (IOD). Pełnomocnicy ds. bezpieczeństwa informacji.

PROWADZĄCY:

przedsiębiorca, doradca biznesowy i samorządowy, bezpartyjny społecznik, autor książki „Skała. Fundament dobrej gminy”. Do 2024 roku pełnił funkcję Burmistrza Miasta i Gminy Skała, a od 2024 r. jest Pełnomocnikiem ds. legislacji w Unii Miasteczek Polskich, reprezentując organizację w grupach roboczych lub komisjach sejmowych i senackich w obszarach cyfryzacji i cyberbezpieczeństwa administracji. Od 2024 roku pełni funkcję CTO w startupie RatePRO wdrażającym rozwiązania AI oraz automatyzacje w samorządzie i biznesie. Jest doradcą biznesowym i samorządowym, specjalizuje się w tematyce samorządowej, cyfryzacji oraz wdrażaniu automatyzacji i sztucznej inteligencji w sektorze publicznym i biznesie. Przez ponad dekadę (2006–2018), prowadził agencję reklamy internetowej, realizując kampanie dla największych marek, m.in. Allegro, Ford, Nissan, BMW, LOT, Hestia, Tchibo czy Lufthansa. Prowadzi i moderuje ogólnopolskie konferencje i kongresy, w tym m.in. Krynica Forum, Forum Miasteczek Polskich, Samorządowe Forum Kapitału i Finansów, Kongres Zarządzania Administracją Samorządową, Smart City w Łodzi i Rzeszowie czy Konferencje „Miasta w Internecie”.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Cyberbezpieczeństwo w administracji samorządowej - praktyczne strategie ochrony danych i przeciwdziałania atakom

	Szkolenie **w formie stacjonarnej w siedzibie FRDL MISTiA** **Kraków, ul. Floriańska 31 - I piętro**
	27 marca 2026 r. **Godz. 9:00 – 14:00**
	Cena: 625 PLN netto/os. **Przy zgłoszeniach do 13 marca 2026 r. cena wynosi: 599 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.
CENA zawiera:	☑ **Materiały szkoleniowe w formie elektronicznej** ☑ **Zaświadczenie uczestnictwa** ☑ **Przerwę kawową oraz poczęstunek** ☑ **Doskonała lokalizacja w centrum Krakowa** ☑ **Możliwość konsultacji z wykładowcą po szkoleniu** ☑ **Wymianę doświadczeń z innymi uczestnikami szkolenia**
DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego, MISTiA ul. Floriańska 31, 31-019, Kraków **Weronika Zwolska,** specjalistka ds. szkoleń **+48 12 623 72 44, 575 850 930,** szkolenia@mistia.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 przesłanie faktury na adres mailowy: ……

Proszę o przesłanie certyfikatu 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.mistia.org.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Zgłoszenia prosimy przesyłać do 23 marca 2026 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 _____