Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
22 stycznia 2026 r.

PODSTAWY CYBERBEZPIECZEŃSTWA DLA PRACOWNIKÓW JEDNOSTEK ADMINISTRACJI PUBLICZNEJ

WAŻNE INFORMACJE:

- W 2023 r. weszła w życie nowa dyrektywa NIS2 dotycząca zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w krajach Unii Europejskiej, a w najbliższym czasie wejdzie w życie nowa ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) jako krajowa implementacja dyrektywy. Wprowadzane zmiany mają istotny wpływ na dotychczasowo stosowaną praktykę w jednostkach, wobec czego aktualizacja wiedzy pracowników, kierowników i dyrektorów, a szczególnie najwyższego kierownictwa jednostek samorządu terytorialnego oraz osób zajmujących na co dzień ochroną informacji i cyberbezpieczeństwem w tym obszarze ma kluczowe znaczenia dla zapewnienia skutecznej ochrony informacji w urzędzie oraz zgodności z aktualnymi wymaganiami w tym także RODO i KRI. Warto pamiętać, że w projekcie nowej ustawy KSC, to **najwyższe kierownictwo ponosi odpowiedzialność** za wdrożenie środków cyberbezpieczeństwa **nawet jeśli te zadania deleguje na innych.** A to będzie bardzo ważna zmiana w codziennej ochronie zasobów informacyjnych urzędów. Dodatkowo Najwyższa Izba Kontroli prowadzi kontrole w jst w całym kraju, które przynoszą bardzo zaskakujące wyniki np. dużego braku świadomości cyberzagrożeń wśród pracowników jst i to niezależnie od wielkości jednostki.
- **Podczas proponowanego szkolenia:**
  - Krok po kroku omówimy zagadnienia związane z cyberbezpieczeństwem w jst oraz jednostkach podległych i roli kadry zarządzającej w zakresie rekomendowanym w powyższym projekcie oraz dyrektywie NIS2 i planowanej ustawie o KSC.
  - Przeanalizujemy występujące cyberzagrożenia i ich konsekwencje.
  - Przypominamy procedury, jakie w zakresie cyberbezpieczeńtwa powinny być wdrożone w jednostce oraz wskażemy, na co w ich zapisach szczególnie zwracać uwagę.
  - Zaprezentujemy zadania i obowiązki jednostek ze szczególnym uwzględnieniem zgłaszania incydentów.
  - Prezentowane zagadnienia prawne będziemy popierać licznymi przykładami z praktyki dla lepszego zobrazowania omawianych regulacji i zasad postępowania.

CELE I KORZYŚCI:

- Dowiesz się:
  - Kto ponosi odpowiedzialność za stan cyberbezpieczeństwa w urzędzie?
  - Czy wdrażane przez jst zabezpieczenia faktycznie działają?
  - Czy kadra zarządzająca zdaje sobie sprawę ze swojej roli w procesie ochrony informacji?
  - Czy pracownicy wiedzą, jak zgłaszać incydenty i dlaczego to jest tak ważne?
  - Czym jest zapewnienie ciągłości działania i zarządzanie incydentami?
- Poznasz główne wymagania formalno-prawne, jakie dotyczą cyberbezpieczeństwa w jst i jednostkach podległych wynikające z dyrektywy NIS2 i nowelizacji KSC oraz RODO i KRI.
- Dowiesz się, jak istotną rolę kadry zarządzającej w zapewnieniu skutecznej ochrony informacji.
- Poznasz zasady skutecznego zarządzania ryzykiem i incydentami bezpieczeństwa w jst.
- Dowiesz się, jak skutecznie nadzorować procesy związane z bezpieczeństwem informacji oraz jak budować kulturę bezpieczeństwa w urzędzie.
- Poznasz sposoby skutecznego zwiększania świadomości cyberzagrożeń wśród pracowników.
- Zapoznasz się z przykładowymi cyberatakami na jst oraz ich konsekwencjami, a także dobrymi praktykami minimalizowania tych konsekwencji.
- Dowiesz się, jakie są najczęstsze błędy popełniane przez jst w zakresie cyberbezpieczeństwa, które wskazywane są podczas kontroli np. NIK oraz testów i audytów bezpieczeństwa.

PROGRAM:

1. Wykorzystywanie sztucznej inteligencji (AI) w dezinformacji i oszustwach internetowych – przykłady.

2. Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa w instytucji publicznej:
   - Jakie mamy obowiązki w naszej organizacji związane z ochroną informacji: RODO, KRI, NIS2/KSC, …?
   - Wewnętrzne polityki i procedury bezpieczeństwa w ramach SZBI.
3. Czy człowiek to najsłabsze ogniwo?
4. Budowanie kultury bezpieczeństwa (świadomości) jest kluczowe dla każdej organizacji.
5. Incydenty bezpieczeństwa:
   - Co to jest incydent?
   - Dlaczego warto zgłaszać incydenty?
   - Kiedy i komu zgłaszać incydenty?
6. Aktualne zagrożenia w cyberprzestrzeni:
   - Typy ataków / główne cyberzagrożenia.
   - Kradzieże i wyłudzenia informacji – przykłady.
   - Jak się bronić?
7. Bezpieczna praca zdalna – dobre praktyki:
   - Dbaj o sprzęt i dostępy do systemów.
   - Zagrożenia dla urządzeń mobilnych i zasady bezpiecznego korzystania.
   - Zabezpieczaj dokumenty przed osobami nieuprawnionymi także w domu.
   - Szyfruj komunikację i dane tam, gdzie tylko można.
   - Używaj dwuskładnikowego uwierzytelnienia zawsze ... jeśli jest to możliwe.
8. Proste i skuteczne metody codziennej ochrony informacji przez pracowników:
   - Kopia bezpieczeństwa wg zasady „3-2-1”.
   - Czy chmurze można zawsze ufać?
   - Szyfrowanie danych.
   - Blokowanie komputera.
   - Fizyczna ochrona urządzeń.
   - Czy pendrive od znajomego może być niebezpieczny? Czy można żyć bez pendrive’a?
   - Dlaczego warto „oszukiwać” i „kłamać” w Internecie?
9. Zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych:
   - Pamiętaj hasło do poczty e-mail.
   - Szyfrowanie załączników do e-maili.
   - Korzystanie z pola „UDW” w programie pocztowym.
   - Bezpieczne hasła do Twoich systemów:
     - Jak tworzyć silne hasła?
     - Jakie hasła zawsze musimy mieć „w głowie”.
     - Menedżery haseł jako właściwe narzędzie do skutecznego zarządzania hasłami. Przykłady
10. Dwuskładnikowe uwierzytelnienie (2FA/MFA) to już standard w pracy i życiu prywatnym:
    - Smsy.
    - Aplikacje.
    - Klucze sprzętowe (U2F).
11. Wycieki i kradzieże haseł:
    - Jak sprawdzić, czy moje hasła wyciekły? Przykładowe serwisy.
    - Co zrobić, gdy moje hasła wycieką?
12. Phishing i Ransomware jako największe zagrożenia dla każdej organizacji:
    - Jak odróżnić fałszywą korespondencję e-mail przychodzącą do naszej organizacji?
    - Jak odróżnić fałszywą korespondencję e-mail przychodzącą do organizacji? Przykłady.
13. Pytania / Dyskusja.

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:

Audytor, trener, doradca. Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń. Audytor normy ISO/IEC 27001. Prowadzi audyty, szkolenia i konsultacje z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa oraz budowania kultury ochrony informacji.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Podstawy cyberbezpieczeństwa dla pracowników jednostek administracji publicznej

	Szkolenie będziemy realizowali **w formie webinarium on line**.
	**22 stycznia 2026 r.** **Szkolenie w godzinach 10:00-14:30**
	**Cena: 479 PLN netto/os.** Przy zgłoszeniach do **8 stycznia 2026 r.** cena wynosi: **429 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.
CENA zawiera:	udział w profesjonalnym szkoleniu on-line z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.
DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego; Świętokrzyskie Centrum ul. Sienkiewicza 78, IV piętro, 25-501 Kielce tel. 41 344 66 30, 533-884-987, centrum@frdl.kielce.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.frdl.kielce.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.kielce.pl do 15 stycznia 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 _____