Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
23 maja 2025 r.

CYBERBEZPIECZEŃSTWO W JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO – OCHRONA DANYCH I SYSTEMÓW IT W ŚWIETLE PRZEPISÓW NIS2 I RODO

INFORMACJE O SZKOLENIU:

Współczesne jednostki samorządu terytorialnego stają w obliczu coraz większych wyzwań związanych z cyberbezpieczeństwem. Rosnąca liczba ataków hakerskich, phishingu oraz wycieków danych osobowych wymusza na administracji publicznej podjęcie skutecznych działań na rzecz ochrony informacji i infrastruktury IT.

Zapraszamy na kompleksowe szkolenie, którego celem jest podniesienie poziomu wiedzy oraz kompetencji zarządzających i pracowników odpowiedzialnych za bezpieczeństwo informacji. Szkolenie uwzględnia najnowsze regulacje prawne, w tym dyrektywę NIS2, ustawę KSC, rozporządzenie KRI oraz RODO, a także przedstawia najlepsze praktyki w zakresie ochrony danych i reagowania na incydenty. Główne obszary, które zastaną omówione podczas realizacji Webinarium to:

- Wprowadzenie do cyberbezpieczeństwa: podstawowe pojęcia, zagrożenia i trendy.
- Ramy prawne i obowiązki kierownictwa w zakresie ochrony danych.
- Tworzenie polityki zarządzania cyberbezpieczeństwem.
- Audyty, monitorowanie i reagowanie na incydenty.
- Integracja cyberbezpieczeństwa z wymogami RODO.

CELE I KORZYŚCI:

- Dowiesz się, jakie są najnowsze zagrożenia cybernetyczne i jak skutecznie im przeciwdziałać w jednostkach samorządu terytorialnego.
- Uzyskasz informacje na temat obowiązujących przepisów prawnych (NIS2, KSC, KRI, RODO) oraz ich wpływu na funkcjonowanie instytucji publicznych.
- Nauczysz się, jak wdrażać polityki i procedury cyberbezpieczeństwa, aby skutecznie chronić dane i systemy IT w swojej organizacji.
- Zdobędziesz umiejętności pozwalające na identyfikację i reagowanie na incydenty związane z naruszeniami bezpieczeństwa.
- Uzyskasz kompetencje w zakresie współpracy z Inspektorem Ochrony Danych oraz zespołami IT w celu zapewnienia zgodności z regulacjami prawnymi.
- Poznasz najlepsze praktyki, które pozwolą na skuteczne przeprowadzanie audytów i wdrażanie działań korygujących w obszarze bezpieczeństwa informacji.
- Nauczysz się, jak skutecznie zarządzać ryzykiem i minimalizować konsekwencje cyberataków.

PROGRAM:

1. **Wprowadzenie do cyberbezpieczeństwa:**
   a. Definicja i znaczenie: Co to jest cyberbezpieczeństwo i dlaczego jest kluczowe w środowisku jednostek publicznych, w tym jednostek organizacyjnych organów prowadzących.
   b. Identyfikacja zagrożeń: Przegląd najczęstszych zagrożeń cybernetycznych, ataków hakerskich, phishingu oraz ich wpływu na funkcjonowanie instytucji publicznych.
   c. Aktualne trendy: Omówienie najnowszych trendów i wyzwań w zakresie cyberbezpieczeństwa.
2. **Ramy prawne i odpowiedzialność kierownictwa:**
   a. Obowiązujące przepisy: Szczegółowy przegląd ustaw i rozporządzeń:
      – Dyrektywa NIS2 - europejski akt prawny w zakresie cyberbezpieczeństwa.
      – Ustawa KSC – kluczowe aspekty dotyczące bezpieczeństwa cybernetycznego.
      – Rozporządzenie KRI – specyfika i wymogi dla jednostek publicznych.
      – RODO i bezpieczeństwo danych osobowych.
      – Norma ISO27001: bezpieczeństwo informacji.
   b. Odpowiedzialność zarządzających: rola i odpowiedzialność dyrektorów oraz członków kadry zarządzającej w kontekście przestrzegania przepisów.
   c. Współpraca z Inspektorem Ochrony Danych: Rola IOD, zasady współpracy z działem IT, osobami zarządzającymi cyberbezpieczeństwem oraz najlepsze praktyki w zakresie monitorowania i raportowania naruszeń.
3. **Budowanie Systemu Zarządzania Cyberbezpieczeństwem:**
   a. Diagnoza stanu bezpieczeństwa: Metody oceny ryzyka oraz identyfikacja kluczowych zasobów i danych wymagających ochrony.
   b. Tworzenie polityk i procedur: Wdrażanie polityk bezpieczeństwa, procedur reagowania na incydenty oraz planów ciągłości działania.

c. Techniczne i organizacyjne środki ochrony: Przykłady narzędzi, technologii oraz rozwiązań wspierających bezpieczeństwo infrastruktury IT.
d. Szkolenia i podnoszenie świadomości: organizacja szkoleń dla pracowników i uczniów, kampanie informacyjne oraz symulacje incydentów.

4. **Audyty i Monitorowanie Systemu Bezpieczeństwa:**
   a. Znaczenie audytów: rola audytów wewnętrznych i zewnętrznych w ocenie skuteczności wdrożonych środków.
   b. Przygotowanie do audytu: kluczowe aspekty, na które audytorzy zwracają uwagę, oraz jak przygotować placówkę do kontroli.
   c. Analiza wyników audytu: interpretacja raportów, wdrażanie rekomendacji oraz ciągłe doskonalenie systemu zarządzania cyberbezpieczeństwem.
5. **Odpowiedzialność i rola Uczestników szkolenia w Instytucjach Publicznych:**
   a. Inspektor Ochrony Danych (IOD):
      – Monitorowanie zgodności z RODO i przepisami krajowymi w urzędach.
      – Doradztwo i prowadzenie rejestrów, szkoleń, audytów.
      – Współpraca z organem nadzorczym, raportowanie naruszeń.
   b. Kadra kierownicza instytucji:
      – Budowanie świadomości wśród pracowników, wspieranie inicjatyw z zakresu cyberbezpieczeństwa.
      – Zapewnienie odpowiednich zasobów (budżet, personel, narzędzia).
      – Odpowiedzialność administracyjna, karna i reputacyjna za naruszenia.
   c. Administratorzy systemów informatycznych:
      – Implementacja i utrzymanie rozwiązań technicznych.
      – Cykliczne przeglądy systemów i aktualizacje zabezpieczeń.
      – Wsparcie w sytuacjach incydentów i współpraca z IOD oraz zespołem reagowania.
   d. Osoby zarządzające cyberbezpieczeństwem (np. CSO/CISO):
      – Definiowanie strategii bezpieczeństwa w administracji publicznej.
      – Współpraca z IOD i innymi działami w zakresie monitorowania ryzyka.
      – Ustalenie procedur zarządzania incydentami i koordynacja działań obronnych.
6. **Reagowanie na incydenty i naruszenia ochrony danych:**
   a. Definiowanie incydentu i naruszenia w sektorze publicznym:
      – Przykłady naruszeń danych osobowych w instytucjach (wyciek danych obywateli, ataki na ePUAP lub lokalne systemy).
      – Różnica między incydentem cyberbezpieczeństwa a naruszeniem ochrony danych osobowych.
   b. Procedura obsługi incydentu:
      – Tworzenie planu reagowania (Incident Response Plan).
      – Zgłaszanie incydentów do właściwych organów (CSIRT poziomu krajowego/branżowego, UODO).
      – Komunikacja z interesariuszami (obywatele, media, instytucje nadrzędne).
   c. Działania po incydencie:
      – Analiza przyczyn (root cause analysis) i wnioski na przyszłość.
      – Aktualizacja polityk, procedur i wdrażanie poprawek technicznych.
      – Kontrola zgodności z RODO i przepisami krajowymi (raporty pokontrolne).
7. **Integracja RODO z Cyberbezpieczeństwem:**
   a. Powiązania między RODO a bezpieczeństwem IT: jak przepisy RODO wpływają na zarządzanie danymi osobowymi i systemami informatycznymi.
   b. Wymogi RODO: omówienie obowiązków związanych z przetwarzaniem danych, monitorowaniem dostępu oraz raportowaniem naruszeń.
   c. Przykłady i studia przypadków: analiza realnych sytuacji, w których niedostateczne zabezpieczenia wpłynęły na naruszenie ochrony danych.

ADRESACI:

- Osoby funkcyjne w urzędach - dyrektorzy, naczelnicy wydziałów/referatów, osoby odpowiedzialne za bezpieczeństwo systemów informatycznych tzw. ASI, Inspektorzy Ochrony danych, pełnomocnicy SZBI, audytorzy wewnętrzni w urzędach;
- Dyrektorzy/kierownicy jednostek organizacyjnych, IOD w tych jednostkach, IT w tych jednostkach;
- Osoby odpowiedzialne za zarządzanie bezpieczeństwem w jednostkach budżetowych;
- Kierownictwo urzędów: wójtowie, burmistrzowie, starości i ich zastępcy.

PROWADZĄCY:

Nieetatowy współpracownik Wyższej Szkoły Nauk Pedagogicznych w Warszawie, audytor w zakresie realizacji wymagań zgodnych z KRI oraz audytor wiodący ISO 27001, obecnie zatrudniony jako inspektor ochrony danych w jednostkach samorządu terytorialnego, prelegent z wieloletnim doświadczeniem na szkoleniach z zakresu ochrony danych osobowych w jednostkach sektora publicznego. Wykładowca ceniony i polecany przez członków Forum Ochrony Danych działającego przy FRDL.
Audytor wewnętrzny bezpieczeństwa informacji normy IOS27001, absolwent studiów podyplomowych na kierunku Inspektor Ochrony Danych. Aktywny członek stowarzyszenia inspektorów ochrony danych (SABI). Posiada doświadczenie w zakresie współpracy z administracją publiczną pełniąc funkcję inspektora ochrony danych oraz obsługując naruszenia ochrony danych. Prowadzi audyty ochrony danych osobowych, audyty bezpieczeństwa systemów informatycznych oraz szkolenia dla pracowników, których tematyka związana jest z danymi osobowymi, prywatnością a także bezpieczeństwem informacji.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Cyberbezpieczeństwo w jednostkach samorządu terytorialnego – ochrona danych i systemów IT w świetle przepisów NIS2 i RODO

	Szkolenie będziemy realizowali **w formie webinarium on line**.
23 maja 2025 r.	**Szkolenie w godzinach 9:30-13:30**
	Cena: 449 PLN netto/os. UWAGA! Przy zgłoszeniu na szkolenie do **5 maja 2025 r.** cena: **419 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 Podkarpacki Ośrodek Samorządu Terytorialnego ul. Kolejowa 1, 35 – 073 Rzeszów tel. 17 862 69 64 **post@frdl.rzeszow.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.rzeszow.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.rzeszow.pl do 19 maja 2025 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 _____