Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ONLINE
14 września 2026

CYBERBEZPIECZEŃSTWO W INSTYTUCJI OKIEM PRAKTYKA— NOWELIZACJA KSC I DYREKTYWA NIS2. WDROŻENIE I ZARZĄDZANIE SYSTEMEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI) W JEDNOSTCE

WAŻNE INFORMACJE:

- **Dynamiczny wzrost liczby cyberataków oraz nowe obowiązki wynikające z Dyrektywy NIS2 i nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC) stawiają przed jednostkami sektora publicznego nowe wymagania w zakresie ochrony informacji i zarządzania bezpieczeństwem. Wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) przestaje być wyłącznie elementem dobrych praktyk, a staje się jednym z kluczowych obowiązków organizacyjnych, mających zapewnić odporność instytucji na incydenty cyberbezpieczeństwa.**
- Jednocześnie skuteczne zarządzanie bezpieczeństwem informacji wymaga nie tylko wdrożenia odpowiednich rozwiązań technicznych, lecz także właściwego określenia odpowiedzialności kierownictwa, przeprowadzenia analizy ryzyka, opracowania wymaganej dokumentacji oraz zapewnienia zgodności z przepisami KSC, RODO, KRI. Szczególnego znaczenia nabiera również budowanie świadomości pracowników, właściwe reagowanie na incydenty oraz przygotowanie organizacji do audytów i kontroli w obszarze cyberbezpieczeństwa.
- **Podczas proponowanego szkolenia prowadzący omówi nie tylko praktyczne aspekty wdrażania i utrzymania SZBI, ale także wskaże konkretne rozwiązania, pozwalające skutecznie zarządzać bezpieczeństwem informacji, ograniczać ryzyko cyberataków oraz prawidłowo realizować obowiązki, wynikające z najnowszych przepisów prawa.**

CELE I KORZYŚCI:

- Usystematyzowanie i pogłębienie wiedzy uczestników w zakresie obowiązków, wynikających z dyrektywy NIS2, nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC) oraz pozostałych regulacji dotyczących bezpieczeństwa informacji w jednostce.
- Przygotowanie skutecznego wdrożenia i zarządzania Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z wymaganiami normy ISO 27001 oraz obowiązującymi przepisami prawa.
- Doskonalenie umiejętności identyfikacji, analizy i ograniczania ryzyka cyberzagrożeń, w tym stosowania odpowiednich zabezpieczeń organizacyjnych, technicznych i proceduralnych w jednostce.
- Przedstawienie zasad opracowania i utrzymania dokumentacji SZBI, prowadzenia analizy ryzyka, przygotowania deklaracji stosowalności (SoA) oraz realizacji audytów wewnętrznych i przeglądów zarządzania.
- Nabycie kompetencji w zakresie bezpieczeństwa informacji i organizacji procesów cyberbezpieczeństwa, zarządzania incydentami oraz współpracy z dostawcami usług IT.
- Wskazanie praktycznych rozwiązań, umożliwiających zapewnienie zgodności organizacji z wymaganiami KSC, NIS2, RODO, KRI i ISO 27001, a także ograniczenie ryzyka naruszeń bezpieczeństwa informacji i skuteczne przygotowanie do audytów oraz kontroli.

PROGRAM:

I. Otoczenie prawne SZBI w organizacji:

1. Najczęstsze cyberzagrożenia w administracji publicznej — dane statystyczne z raportów NASK, CERT Polska. Typowe wektory ataków i sektorowe podatności.

2. Regulacje prawne, wzajemne zależności i hierarchia wymogów:
   - Dyrektywa NIS2,
   - Dyrektywa CER,
   - RODO,
   - ustawa KSC po nowelizacji,
   - Rozporządzenie KRI, ISO 27001.

II. Etapy wdrażania SZBI zgodnie z ISO 27001:

1. Obowiązki organizacji — wdrożenie SZBI, dokumentacja bezpieczeństwa, rola gestora systemu, odpowiedzialność ustawowa, audyty i kontrole ds. cyberbezpieczeństwa.
2. SZBI w praktyce: czym jest, jakie korzyści przynosi, cykl PDCA. Mapowanie wymogów KSC (art. 8 i 10) z ISO 27001. Tabela zgodności, gap analysis.
3. Etapy wdrożenia SZBI:
   - analiza kontekstu,
   - szacowanie ryzyka,
   - deklaracja stosowalności (SoA),
   - zabezpieczenia wg załącznika A ISO 27001,
   - audyt wewnętrzny,
   - przegląd zarządzania — rola kadry kierowniczej jako właścicieli ryzyk.

III. Cyberzagrożenia — identyfikacja, unikanie i reagowanie:

1. Zabezpieczenia techniczne i infrastrukturalne:
   - endpoint security (EDR/XDR),
   - silne hasła i MFA,
   - bezpieczeństwo sieci i poczty elektronicznej,
   - cyberhigiena.
2. Bezpieczeństwo w umowach z dostawcami IT — klauzule i wymogi.
3. Świadomy przełożony w procesie przetwarzania informacji:
   - szyfrowanie danych,
   - zasada czystego ekranu i biurka,
   - kontrola dostępu,
   - praca zdalna — procedury i najczęstsze błędy pracowników,
   - skutkujące incydentami.
4. Studium przypadku.

IV. Dyskusja, odpowiedzi na pytania.

ADRESACI:

Kadra kierownicza administracji publicznej, w tym jst, sekretarze jst oraz osoby odpowiedzialne za bezpieczeństwo informacji, IT i cyberbezpieczeństwo, IOD, audytorzy, compliance, właściciele procesów oraz osoby odpowiedzialne za ciągłość działania, osoby wyznaczone do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa i obsługi obowiązków KSC.

PROWADZĄCY:

Doświadczony trener, szkoleniowiec, przedsiębiorca, praktyk. Wdrożeniowiec platform, systemów i narzędzi ICT. Realizator projektów z obszaru: kompetencji cyfrowych, cyberbezpieczeństwa, bezpiecznej pracy w sieci. Prowadził szkolenia z tematyki ochrony danych osobowych, RODO, e-doręczeń, dostępności cyfrowej, transformacji cyfrowej, elektronicznego zarządzania dokumentacją (EZD), podpisu elektronicznego (aspektów technicznych, zmian w k.p.a.). Posiada ponad 10 lat doświadczenia w obszarach cyfryzacji i procesów digital. Zrealizował ponad 6000 godzin szkoleniowych w ramach edukacji, wdrożenia, konsultingu merytorycznego i technicznego. Przeprowadził szkolenia warsztatowe m.in. dla Kancelarii Prezesa Rady Ministrów, Ministerstwa Cyfryzacji, Ministerstwa Edukacji, Ministerstwa Finansów, Ministerstwa Zdrowia, Państwowej Inspekcji Pracy, Agencji Rezerw Strategicznych, Agencji Restrukturyzacji i Modernizacji Rolnictwa, Agencji Mienia Wojskowego.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE
KARTA ZGŁOSZENIA

Cyberbezpieczeństwo w instytucji okiem praktyka— nowelizacja KSC i dyrektywa NIS2. Wdrożenie i zarządzanie systemem zarządzania bezpieczeństwem informacji (SZBI) w jednostce

	Szkolenie będziemy realizowali **w formie webinarium online**.
	14 września 2026 r. **Szkolenie w godzinach 9:00-13:00**
	Cena: 479 PLN netto/os. Przy zgłoszeniu **do 31 sierpnia 2026 r.** cena wynosi: **449 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.
CENA zawiera:	udział w profesjonalnym szkoleniu online 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

(dane do faktury)
Nazwa i adres nabywcy
NIP

Nazwa i adres odbiorcy
NIP

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 ☐

Faktura zostanie wystawiona jako faktura ustrukturyzowana w Krajowym Systemie e-Faktur (KSeF).

Uwagi: ……

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 www.frdl.rzeszow.pl do 8 września 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 faktury w KSeF.

Podpis osoby upoważnionej _____