Sesja konsultacyjno szkoleniowa Forum Sekretarzy

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa 2026. Obowiązki JST, NIS2, KSC i reagowanie na incydenty

23 czerwca 2026 r. 10:00 do 14:00

spotkanie online i stacjonarnie, formuła hybrydowa

Cyberbezpieczeństwo przestało być wyłącznie zadaniem informatyków. W praktyce JST dotyczy ono kierownictwa, sekretarzy, pracowników merytorycznych, osób odpowiedzialnych za organizację pracy urzędu, obieg informacji, dokumentowanie działań oraz reakcję na incydenty.

Czerwcowa sesja Forum porządkuje najważniejsze obowiązki wynikające z NIS2 oraz KSC I pokazuje, jak przełożyć je na realne procedury w urzędzie. Uczestnicy otrzymają praktyczne wskazówki dotyczące rozpoznawania zagrożeń, reagowania na incydenty, współpracy z dostawcami IT oraz przygotowania jednostki do audytu zgodności.

Ekspert: ekspert w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji oraz zarządzania kryzysowego, posiadający wieloletnie doświadczenie zawodowe w administracji państwowej. Obecnie na co dzień realizuje usługi dotyczące zarządzania cyberbezpieczeństwem, audytów, wdrażania bezpieczeństwa informacji oraz szkoleń.

Spotkanie będzie realizowane w formule hybrydowej. Część stacjonarna odbędzie się w wieżowcu przy ul. T. Chałubińskiego 8, piętro 10, a część online na platformie ZOOM.

Zachęcam do udziału w najbliższym spotkaniu Forum.

Michał Wójcik
Dyrektor ośrodka regionalnego Fundacji
Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego w Warszawie

Sesja konsultacyjno szkoleniowa Forum Sekretarzy

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa 2026. Obowiązki JST, NIS2, KSC i reagowanie na incydenty

23 czerwca 2026 r. 10:00 do 14:00

spotkanie online i stacjonarnie, formuła hybrydowa

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa oraz wdrażanie wymogów NIS2 oznaczają dla jednostek samorządu terytorialnego konieczność uporządkowania procesów, procedur, odpowiedzialności i dokumentacji. To nie jest temat na odkładanie do szuflady z napisem „informatyka", bo ta szuflada zwykle potem bardzo głośno się domyka.

Podczas sesji uczestnicy przeanalizują obowiązki JST, odpowiedzialność kierownictwa, plan wdrożenia wymogów w gminie, zasady edukowania pracowników oraz praktyczne reagowanie na incydenty. Program opiera się na przykładach, scenariuszach i błędach znanych z realnej pracy administracji publicznej.

Cele i korzyści z udziału w sesji:

Udział w sesji pozwoli zdobyć wiedzę wdrożeniową, a nie wyłącznie teoretyczną. Uczestnicy uporządkują wymagania prawne i organizacyjne, poznają dobre praktyki oraz konkretne procedury, które pomagają ograniczyć ryzyko cyberincydentów w urzędzie.

Sekretarzu, dzięki szkoleniu:

- ✓ rozpoznasz najczęstsze zagrożenia dotyczące JST, w tym phishing, ransomware, wycieki danych oraz ataki na systemy rejestrów
- ✓ zrozumiesz, jakie obowiązki nakładają na JST przepisy związane z NIS2 i KSC
- ✓ poznasz zakres odpowiedzialności kierownictwa oraz znaczenie dokumentowania działań
- ✓ dowiesz się, jak przygotować urząd do audytu zgodności i kontroli
- ✓ otrzymasz praktyczny plan działań wdrożeniowych dla gminy
- ✓ przećwiczysz reakcję na incydent oraz poznasz najczęstsze błędy popełniane w pierwszych godzinach po ataku
- ✓ dowiesz się, jak edukować pracowników urzędu, aby ograniczać ryzyko błędów ludzkich

Program sesji:

I. Wprowadzenie do NIS2 i KSC:

1.1. Geneza i cele dyrektywy NIS2 oraz ustawy o KSC.
1.2. Stan prawny NIS2 i KSC po nowelizacji.
1.3. Zakres podmiotowy, które jednostki samorządu podlegają regulacjom.
1.4. System zarządzania bezpieczeństwem informacji ISO 27001.

II. Odpowiedzialność kierownictwa JST:

2.1. Osobista odpowiedzialność.
2.2. Obowiązki zatwierdzania i nadzorowania polityk Bezpieczeństwa.
2.3. Dokumentowanie działań, jak przygotować się na kontrolę.
2.4. Sankcje i kary, co grozi jednostce i osobom funkcyjnym.

III. Plan wdrożenia NIS2 w gminie:

3.1. Przykładowy harmonogram wdrożenia.

3.2. Minimalny zespół wdrożeniowy, kogo zaangażować w urzędzie.
3.3. Współpraca z dostawcami IT i podmiotami zewnętrznymi.
3.4. Lista kontrolna działań.

IV. Wymogi wobec pracowników urzędu:

4.1. Obowiązek szkoleń z cyberbezpieczeństwa.
4.2. Jak skutecznie edukować pracowników administracji.
4.3. Typowe błędy urzędników, przykłady z praktyki.
4.4. Ćwiczenie, symulacja phishingu w urzędzie.

V. Audyty, incydenty i reagowanie:

5.1. Jak JST powinna przygotować się do audytu zgodności NIS2.
5.2. Typowe zagrożenia dla gmin, ransomware, phishing, ataki na systemy rejestrów.
5.3. Procedura zgłaszania incydentu do CSIRT NASK.
5.4. Pierwsze 24 do 72 godzin po ataku.

VI. Podsumowanie.

Prowadzący sesję:

ekspert w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji oraz zarządzania kryzysowego, posiadający wieloletnie doświadczenie zawodowe w administracji państwowej.

Obecnie Pan Piotr Tchorzewski odpowiada za realizację usług z obszaru zarządzania cyberbezpieczeństwem, audytów, wdrażania bezpieczeństwa informacji oraz szkoleń w przedmiotowym zakresie.

Wcześniej wiele lat pracował w administracji państwowej, zajmując kolejno stanowiska specjalisty, naczelnika oraz dyrektora. Posiada wykształcenie wyższe w zakresie zarządzania cyberbezpieczeństwem, a także uprawnienia Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO/IEC 27001.

Od 2006 r. prowadzi szkolenia, warsztaty i wykłady z zakresu bezpieczeństwa informacji oraz cyberbezpieczeństwa. Jest autorem lub współautorem artykułów i publikacji zwartych dotyczących bezpieczeństwa informacji.

Łączy doświadczenie menedżerskie, audytorskie i szkoleniowe z praktyką operacyjną, co zapewnia wysoki poziom merytoryczny oraz praktyczny charakter prowadzonych szkoleń.

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIOWA		
Sesja konsultacyjno szkoleniowa Forum Sekretarzy nt.:		
23 czerwca 2026 r. Szkolenie w godzinach 10:00 do 14:00		
Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa 2026. Obowiązki JST, NIS2, KSC i reagowanie na incydenty		
spotkanie online na platformie ZOOM oraz stacjonarnie w Warszawie, ul. T. Chałubińskiego 8, piętro 10		
Koszt udziału w spotkaniu dla osoby niezrzeszonej w Forum wynosi 459 PLN w formule online oraz 690 PLN w formule stacjonarnej. W przypadku członka Forum koszt wynosi 250 PLN. Cena obejmuje: udział w profesjonalnej sesji konsultacyjno szkoleniowej, materiały szkoleniowe, możliwość konsultacji z trenerem i uczestnikami sesji.		
Forma udziału w zajęciach, proszę zaznaczyć właściwe		**Stacjonarna ☐ Online ☐**
DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego, Centrum Mazowsze ul. Jelinka 6, 01 646 Warszawa, tel. 517 515 717, szkolenia@frdl.org.pl	
Nazwa jednostki		
Dane Nabywcy Faktury		
NIP Nabywcy		
Dane odbiorcy faktury		
NIP odbiorcy, KSeF		
Imię i nazwisko uczestnika		
Kontakt: telefon i adres poczty elektronicznej		
Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70 procent ze środków publicznych, proszę zaznaczyć właściwe		**TAK ☐** **NIE ☐**
Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń FRDL 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. Termin zgłoszeń wymaga potwierdzenia przez Organizatora.		
UWAGA Liczba miejsc ograniczona. O udziale decyduje kolejność zgłoszeń. Zgłoszenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji z udziału najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za udział niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.		

Podpis osoby upoważnionej _____