

DOLNOŚLĄSKIE FORUM SEKRETARZY.

CYBERBEZPIECZEŃSTWO, NIS-2 /UKSC DLA SEKRETARZY URZĘDÓW MIAST WOJEWÓDZTWA DOLNOŚLĄSKIEGO.

WAŻNE INFORMACJE O FORUM

Zapraszamy na kolejne już w tym roku spotkanie w ramach Dolnośląskiego Forum Sekretarzy, które poświęcone będzie niezwykle istotnemu tematowi – cyberbezpieczeństwu w kontekście nowych regulacji NIS-2 oraz uKSC. W dobie rosnącej liczby zagrożeń w cyberprzestrzeni oraz zmieniających się wymogów prawnych, szczególnie ważne jest, aby urzędy miast i gmin skutecznie przygotowały się na nowe wyzwania.

Podczas szkolenia omówimy kluczowe obowiązki wynikające z regulacji NIS-2 oraz uKSC, w tym identyfikację ryzyk, procedury reagowania na incydenty i obowiązek raportowania. Uczestnicy poznają praktyczne wskazówki dotyczące wdrażania nowych przepisów, a także konsekwencje ich niewypełnienia. Nie zabraknie również przykładów studiów przypadków oraz wymiany doświadczeń.

Szkolenie skierowane jest do sekretarzy urzędów miast i gmin, którzy pragną podnieść poziom bezpieczeństwa w swoich jednostkach, a także wdrożyć dobre praktyki w zakresie ochrony przed cyberzagrożeniami.

Zapraszamy do udziału w tym wyjątkowym wydarzeniu, które łączy nowoczesne technologie z potrzebami współczesnej administracji!

CELE I KORZYŚCI:

- Przekazanie sekretarzom wiedzy na temat regulacji NIS-2 oraz uKSC i ich znaczenia dla zapewnienia cyberbezpieczeństwa w administracji publicznej.
- Wyjaśnienie kluczowych obowiązków i odpowiedzialności urzędów miast i gmin w zakresie ochrony przed zagrożeniami w cyberprzestrzeni.
- Omówienie praktycznych aspektów wdrożenia regulacji NIS-2 w jednostkach administracyjnych, w tym identyfikacji ryzyk, procedur reagowania na incydenty oraz obowiązków raportowych.
- Przedstawienie przykładów dobrych praktyk i narzędzi wspierających cyberbezpieczeństwo, które mogą być wdrażane w urzędach miast i gmin.
- Zwiększenie świadomości sekretarzy w zakresie zarządzania incydentami cyberbezpieczeństwa, od ich identyfikacji po współpracę z zewnętrznymi podmiotami, takimi jak CERT i Policja.
- Uświadomienie sekretarzom znaczenia budowania kultury cyberbezpieczeństwa w urzędach, w tym roli szkoleń i procedur zgodnych z regulacjami NIS-2.
- Inspirowanie do wdrażania innowacyjnych rozwiązań i technologii, które zwiększą odporność na cyberzagrożenia i podniosą efektywność administracji.

PROGRAM:

I. Wprowadzenie do cyberbezpieczeństwa, NIS-2 i uKSC

1. Powitanie uczestników i przedstawienie agendy szkolenia.
2. Podstawowe informacje o NIS-2 i uKSC:
 - Cele i znaczenie regulacji.
 - Rola administracji publicznej w zapewnianiu cyberbezpieczeństwa.
3. Kto podlega regulacjom?
 - Kluczowe podmioty i jednostki.
 - Kryteria uznawania podmiotów za istotne lub kluczowe.
4. Sesja pytań i odpowiedzi.

II. Wymagania i obowiązki wynikające z NIS-2 i uKSC

1. Podstawowe obowiązki urzędów miasta:
 - Identyfikacja ryzyk związanych z cyberbezpieczeństwem.
 - Procedury reagowania na incydenty.
 - Obowiązek raportowania incydentów.
2. Konsekwencje niewypełnienia obowiązków:
 - Sankcje administracyjne i prawne.
 - Reputacyjne skutki incydentów cyberbezpieczeństwa.
3. Praktyczne aspekty wdrożenia NIS-2 w urzędach miasta:
 - Współpraca z CSIRT (zespołami reagowania na incydenty).
 - Tworzenie polityk bezpieczeństwa IT.
4. Przerwa kawowa.

III. Zarządzanie incydentami cyberbezpieczeństwa

1. Definicja incydentu i klasyfikacja:
 - Przykłady najczęstszych zagrożeń.
 - Jak rozpoznawać incydenty w praktyce?
2. Procedury reagowania:
 - Krok po kroku: co zrobić w przypadku wykrycia incydentu?
 - Współpraca z zewnętrznymi podmiotami (np. Policja, CERT).
3. Studium przypadku:
 - Analiza studium przypadku: symulacja incydentu w urzędzie miasta.
 - Omówienie wyników i wspólna dyskusja.

IV. Dobre praktyki i wytyczne

1. Budowanie kultury cyberbezpieczeństwa w urzędzie miasta:
 - Szkolenia i podnoszenie świadomości wśród pracowników.
 - Tworzenie procedur zgodnych z NIS-2.
2. Narzędzia i technologie wspierające cyberbezpieczeństwo:
 - Monitorowanie systemów IT.
 - Zarządzanie tożsamością i dostępem.
3. Checklista wdrożeniowa:
 - Kluczowe kroki do zapewnienia zgodności z NIS-2.
4. Sesja pytań i odpowiedzi.

V. Podsumowanie i zakończenie

1. Najważniejsze wnioski:
 - Podsumowanie kluczowych informacji.
 - Rekomendacje dla sekretarzy urzędów miasta.

ADRESACI:

Członkowie Dolnośląskiego Forum Sekretarzy, Sekretarze niezrzeszeni w Forum, kadra kierownicza zarządzająca zespołami pracowniczymi, jak również osoby, które chcą poszerzyć swą wiedzę z zakresu problematyki będącej przedmiotem szkolenia.

DOLNOŚLĄSKIE FORUM SEKRETARZY. CYBERBEZPIECZEŃSTWO, NIS-2 /UKSC DLA SEKRETARZY URZĘDÓW MIAST WOJEWÓDZTWA DOLNOŚLĄSKIEGO



Szkolenie będziemy realizowali w formie stacjonarnej
Wrocław ul. Piłsudskiego 43, III piętro.



26 marca 2025 r. Szkolenie w godzinach: 10:00-14:00



Cena: członkowie Forum w ramach składki, pozostałe osoby 550 PLN netto/os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera: udział w profesjonalnym szkoleniu z możliwością konsultacji z trenerem, materiały szkoleniowe w wersji elektronicznej, poczęstunek.

DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej im. J. Regulskiego
Ośrodek Kształcenia Samorządu Terytorialnego im. W. Pańki
ul. Piłsudskiego 43, 50-032 Wrocław
ul. Moniuszki 7, 40-005 Katowice
71 344 26 90, 32 206 98 43 szkolenia@okst.pl; milena.dudek@okst.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

Członek FORUM SEKRETARZY TAK NIE

Członek Śląskiego Związku Gmin i Powiatów TAK NIE

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora www.okst.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.okst.pl do 21 marca 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 _____