Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ONLINE
20 sierpnia 2026 r.

NOWE OBOWIĄZKI WYNIKAJĄCE Z USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA (KSC) DLA PODMIOTÓW WAŻNYCH

WDROŻENIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI) I PRZYGOTOWANIE ORGANIZACJI DO REALIZACJI OBOWIĄZKÓW PO WEJŚCIU W ŻYCIE NOWELIZACJI KSC

WAŻNE INFORMACJE O SZKOLENIU:

Szkolenie ma charakter praktyczny. Część prawna wprowadza kontekst, ale zasadnicza część zajęć poświęcona jest temu, co organizacja musi faktycznie wdrożyć, udokumentować i utrzymywać, czyli biorąc udział w szkoleniu można spodziewać się:

- omówienia przepisów i pojęć tylko w zakresie niezbędnym do wdrożenia;
- pracy na przykładach obowiązków: wymóg ustawowy - działanie organizacyjne - dowód wykonania;
- pokazania minimalnej struktury SZBI dla podmiotu ważnego;
- omówienia typowych błędów: sama dokumentacja bez wdrożenia, brak właścicieli procesów, brak rejestrów, brak testów, brak procedury eskalacji incydentów;
- końcowego przejście przez plan działań, który uczestnicy mogą wykorzystać po szkoleniu.

W trakcie szkolenia omówiona zostanie przykładowa lista pierwszych działań wdrożeniowych: potwierdzenie statusu podmiotu, identyfikacja usług i systemów, wyznaczenie odpowiedzialności, przygotowanie procedury incydentowej, analiza luk SZBI oraz harmonogram prac na pierwsze 30, 60 i 90 dni.

Materiały dla uczestników będą obejmować:

- skrótowa checklista samoidentyfikacji podmiotu ważnego;
- mapa obowiązków podmiotu ważnego po nowelizacji KSC;
- spis minimalnej dokumentacji SZBI;
- lista podstawowych rejestrów: aktywa, ryzyka, incydenty, podatności, dostawcy, uprawnienia, szkolenia i działania korygujące;
- prosty plan wdrożenia SZBI do wykorzystania po szkoleniu.

Podstawy prawne

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w brzmieniu po nowelizacji z 2026 r. ISAP - Dz.U. 2026 poz. 20.
- Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Dziennik Ustaw - Dz.U. 2026 poz. 252.
- Materiały informacyjne Ministerstwa Cyfryzacji dotyczące nowelizacji KSC, samoidentyfikacji, terminów i zakresu podmiotowego. gov.pl - baza wiedzy KSC.

CELE I KORZYŚCI:

Udział w szkoleniu daje uczestnikowi tzw. świadomość audytową tzn. pozna:

- jakie są obszary wymagań KRI i uKSC (SZBI) i jak one w praktyce „materializują się” w organizacji,
- jak audytor planuje i wykonuje audyt zgodności (metodyka z ISO/IEC 27001 jako rama pracy, nie kurs audytora),
- jakie dowody są uznawane (dokumenty, rejestry, konfiguracje, logi, zapisy z systemów, testy),
- jak odróżnia się: ustalenia audytowe (UD) vs obserwację (OBS) vs niezgodność (NC) i jak buduje się uzasadnienie oraz działania korygujące.

PROGRAM:

Moduł 1. Wprowadzenie do nowelizacji KSC

1. Cel zmian i powiązanie KSC z dyrektywą NIS2;
2. Nowy podział podmiotów: podmioty kluczowe i podmioty ważne;
3. Najważniejsze obszary obowiązków: SZBI, incydenty, rejestracja, odpowiedzialność kierownictwa i nadzór.

Moduł 2. Kim są podmioty ważne

1. Ogólna charakterystyka podmiotów ważnych i różnica względem podmiotów kluczowych;
2. Samoidentyfikacja: sektor działalności, faktyczny zakres usług, wielkość podmiotu i załączniki do ustawy;
3. Przykładowe sektory, w których mogą występować podmioty ważne, oraz typowe problemy kwalifikacyjne.

Moduł 3. Obowiązki formalne i organizacyjne

1. Wpis do Wykazu KSC albo uzupełnienie danych po wpisie z urzędu;
2. Rola Systemu S46 w komunikacji z CSIRT i organami właściwymi;
3. Wyznaczenie osób odpowiedzialnych, uporządkowanie ról i odpowiedzialności oraz zapewnienie obsługi cyberbezpieczeństwa.

Moduł 4. SZBI jako główny element wdrożenia

1. Czym jest SZBI i dlaczego nie jest wyłącznie dokumentem lub polityką bezpieczeństwa;
2. Powiązanie SZBI z analizą ryzyka, aktywami, usługami, systemami, personelem, dostawcami i ciągłością działania;
3. Minimalny zestaw dokumentów i rejestrów: aktywa, ryzyka, incydenty, dostawcy, dostępy, podatności, szkolenia i działania korygujące;

Moduł 5. Incydenty i współpraca z CSIRT

1. Podstawowe pojęcia: incydent, incydent poważny, podatność i cyberzagrożenie;
2. Wewnętrzna procedura zgłaszania, klasyfikacji i eskalacji zdarzeń;
3. Zgłaszanie incydentów właściwymi kanałami oraz powiązanie z obowiązkami wynikającymi z RODO.

Moduł 6. Odpowiedzialność kierownictwa, personel i szkolenia

1. Odpowiedzialność kierownika podmiotu za organizację i nadzór nad realizacją obowiązków KSC;
2. Rola decyzji zarządczych, budżetu, przeglądów i cyklicznej oceny SZBI;
3. Szkolenia kierownictwa i pracowników, cyberhigiena oraz zasady zgłaszania zdarzeń.

Moduł 7. Dostawcy ICT i łańcuch dostaw

1. Identyfikacja dostawców istotnych dla działania usług i systemów informacyjnych;
2. Ocena ryzyka dostawców oraz minimalne wymagania bezpieczeństwa w umowach i sla;
3. Zgłaszanie incydentów przez dostawców, podwykonawcy, kopie zapasowe, prawo audytu i zakończenie współpracy.

Moduł 8. Dokumentacja, dowody zgodności i przygotowanie do nadzoru

1. Jak dokumentować realizację obowiązków KSC bez tworzenia martwej dokumentacji;
2. Czego może dotyczyć kontrola, audyt albo żądanie organu właściwego;
3. Najczęstsze błędy wdrożeniowe: brak analizy ryzyka, brak właścicieli procesów, brak procedury incydentowej, brak nadzoru nad dostawcami i brak dowodów wykonania.

ADRESACI:

- kadra kierownicza 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:

Prowadzący I - 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.

Prowadzący II - 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

Nowe obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa (ksc) dla podmiotów ważnych. Wdrożenie systemu zarządzania bezpieczeństwem informacji (szbi) i przygotowanie organizacji do realizacji obowiązków po wejściu w życie nowelizacji ksc

Szkolenie będziemy realizowali **w formie webinarium online**.

20 sierpnia 2026 r. **Szkolenie w godzinach 9.00-14.00**

Cena: 479 zł netto/os. Przy zgłoszeniu do 3 sierpnia 2026 r. cena wynosi 449 zł 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, MISTiA
ul. Floriańska 31, 31-019, Kraków
Magdalena Stawiarska, kierownik zespołu ds. szkoleń
tel. +48 12 623 72 44, 575 850 930, szkolenia@mistia.org.pl

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

(dane do faktury)
Nazwa i adres nabywcy
NIP Nabywcy

Nazwa i adres odbiorcy
NIP Odbiorcy

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 ☐

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.mistia.org.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać do 17 sierpnia 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 _____