

CYBERBEZPIECZEŃSTWO W JST

WAŻNE INFORMACJE:

- W 2023 r. weszła w życie dyrektywa NIS2, a w tym roku została uchwalona i weszła w życie (03.04.2026 r.) nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), stanowiąca jej krajową implementację. Nowe przepisy, w sposób istotny, zmieniają dotychczasowe podejście do zarządzania cyberbezpieczeństwem w jednostkach sektora publicznego, w tym w JST. Ustawa KSC znacząco rozszerza zakres obowiązków organizacyjnych, technicznych i raportowych, a także jednoznacznie wskazuje odpowiedzialność najwyższego kierownictwa JST za zapewnienie właściwego poziomu cyberbezpieczeństwa – nawet w przypadku delegowania zadań na pracowników lub podmioty zewnętrzne. W tej sytuacji, aktualizacja wiedzy pracowników, kierowników i dyrektorów, a w szczególności najwyższego kierownictwa JST oraz osób odpowiedzialnych za cyberbezpieczeństwo, ma fundamentalne znaczenie dla zapewnienia zgodności z nowymi wymaganiami prawa, w tym KSC, RODO oraz KRI, a także dla realnego ograniczania ryzyk cybernetycznych. Znaczenie tych zagadnień potwierdzają również wyniki kontroli prowadzonych przez Najwyższą Izbę Kontroli w JST w całym kraju, które wskazują m.in. na niski poziom świadomości cyberzagrożeń wśród pracowników, niezależnie od wielkości podmiotu.
- **Podczas proponowanego szkolenia:**
 - Krok po kroku omówimy zagadnienia związane z cyberbezpieczeństwem w jst oraz jednostkach podległych i roli kadry zarządzającej w zakresie wymaganym w dyrektywie NIS2 i KSC.
 - Przeanalizujemy występujące cyberzagrożenia i ich konsekwencje.
 - Przypominamy procedury, jakie w zakresie cyberbezpieczeństwa powinny być wdrożone w jednostce oraz wskażemy, na co w ich zapisach szczególnie zwracać uwagę.
 - Zaprezentujemy zadania i obowiązki jednostek ze szczególnym uwzględnieniem zgłaszania incydentów.
 - Prezentowane zagadnienia prawne będziemy popierać licznymi przykładami z praktyki dla lepszego zobrazowania omawianych regulacji i zasad postępowania.

CELE I KORZYŚCI:

- Dowiesz się:
 - Kto ponosi odpowiedzialność za stan cyberbezpieczeństwa w urzędzie?
 - Czy wdrażane przez jst zabezpieczenia faktycznie działają?
 - Czy kadra zarządzająca zdaje sobie sprawę ze swojej roli w procesie ochrony informacji?
 - Czy pracownicy wiedzą, jak zgłaszać incydenty i dlaczego to jest tak ważne?
 - Czym jest zapewnienie ciągłości działania i zarządzanie incydentami?
- Poznasz główne wymagania formalno-prawne, jakie dotyczą cyberbezpieczeństwa w jst i jednostkach podległych wynikające z dyrektywy NIS2 i nowelizacji KSC oraz RODO i KRI.
- Dowiesz się, jak istotną rolę kadry zarządzającej w zapewnieniu skutecznej ochrony informacji.
- Poznasz zasady skutecznego zarządzania ryzykiem i incydentami bezpieczeństwa w jst.
- Dowiesz się, jak skutecznie nadzorować procesy związane z bezpieczeństwem informacji oraz jak budować kulturę bezpieczeństwa w urzędzie.
- Poznasz sposoby skutecznego zwiększania świadomości cyberzagrożeń wśród pracowników i kadry.
- Zapoznasz się z przykładowymi cyberatakami na jst oraz ich konsekwencjami, a także dobrymi praktykami minimalizowania tych konsekwencji.
- Dowiesz się, jakie są najczęstsze błędy popełniane przez jst w zakresie cyberbezpieczeństwa, które wskazywane są podczas kontroli np. NIK oraz testów i audytów bezpieczeństwa.

PROGRAM:

1. Wykorzystywanie sztucznej inteligencji (AI) w dezinformacji i oszustwach internetowych – przykłady.
2. Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa w instytucji publicznej:
 - Jakie mamy obowiązki w naszej organizacji związane z ochroną informacji: RODO, KRI, KSC

- Wewnętrzne polityki i procedury bezpieczeństwa w ramach SZBI.
3. Czy człowiek to nadal najsłabsze ogniwo?
 4. Budowanie kultury bezpieczeństwa (świadomości) jest kluczowe dla każdej organizacji.
 5. Incydenty bezpieczeństwa:
 - Co to jest incydent?
 - Dlaczego warto zgłaszać incydenty?
 - Kiedy i komu zgłaszać incydenty?
 6. Aktualne zagrożenia w cyberprzestrzeni:
 - Typy ataków / główne cyberzagrożenia.
 - Kradzieże i wyludzenia informacji – przykłady.
 - Jak się bronić?
 7. Bezpieczna praca zdalna – dobre praktyki:
 - Dbaj o sprzęt i dostępy do systemów.
 - Zagrożenia dla urządzeń mobilnych i zasady bezpiecznego korzystania.
 - Zabezpieczaj dokumenty przed osobami nieuprawnionymi także w domu.
 - Szyfruj komunikację i dane tam, gdzie tylko można.
 - Używaj dwuskładnikowego uwierzytelnienia (2FA/MFA) zawsze ... jeśli jest to możliwe.
 8. Proste i skuteczne metody codziennej ochrony informacji przez pracowników:
 - Kopia bezpieczeństwa wg zasady „3-2-1”.
 - Czy chmurze można zawsze ufać?
 - Szyfrowanie danych.
 - Blokowanie komputera.
 - Fizyczna ochrona urządzeń.
 - Czy pendrive od znajomego może być niebezpieczny? Czy można żyć bez pendrive’a?
 - Dlaczego warto „oszukiwać” i „kłamać” w Internecie?
 9. Zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych:
 - Pamiętaj hasło do poczty e-mail.
 - Szyfrowanie załączników do e-maili.
 - Korzystanie z pola „UDW” w programie pocztowym.
 - Bezpieczne hasła do Twoich systemów:
 - Jak tworzyć silne hasła?
 - Jakie hasła zawsze musimy mieć „w głowie”.
 - Menedżery haseł jako właściwe narzędzie do skutecznego zarządzania hasłami. Przykłady
 10. Dwuskładnikowe uwierzytelnienie (2FA/MFA) to już standard w pracy i życiu prywatnym:
 - Smsy.
 - Aplikacje.
 - Klucze sprzętowe (U2F).
 11. Wycieki i kradzieże haseł:
 - Jak sprawdzić, czy moje hasła wyciekły? Przykładowe serwisy.
 - Co zrobić, gdy moje hasła wyciekną?
 12. Phishing i Ransomware jako największe zagrożenia dla każdej organizacji:
 - Jak odróżnić fałszywą korespondencję e-mail przychodzącą do naszej organizacji?
 - Jak odróżnić fałszywą korespondencję e-mail przychodzącą do organizacji? Przykłady.
 13. Pytania / Dyskusja.

ADRESACI:

- Kadra zarządzająca jst (w tym najwyższe kierownictwo podmiotu): prezydenci, burmistrzowie, wójtowie, starostowie, sekretarze, dyrektorzy, kierownicy.
- Pracownicy działów IT.
- Inspektorzy ochrony danych (IOD).
- Pełnomocnicy ds. bezpieczeństwa informacji.

PROWADZĄCY:

audytor, trener, doradca. Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń. Audytor norm ISO/IEC 27001 i ISO/IEC 22301. Prowadzi audyty, szkolenia i konsultacje z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa oraz budowania kultury ochrony informacji. .

Cyberbezpieczeństwo w JST



Szkolenie będziemy realizowali w formie webinarium online.



15 maja 2026 r.

Szkolenie w godzinach 10:00-14:30



Cena: 479 PLN netto/os. Przy zgłoszeniach do 30 kwietnia 2026 r. cena wynosi: 429 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, 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

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

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 przelać poprzez formularz zgłoszenia na www.mistia.org.pl lub mailem na szkolenia@mistia.org.pl do 11 maja 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 _____