Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ONLINE
16 czerwca 2026 r.

CYBERBEZPIECZEŃSTWO W JST W PRAKTYCE – ZAPOBIEGANIE, REAGOWANIE, ZGODNOŚĆ Z PRZEPISAMI

WAŻNE INFORMACJE O SZKOLENIU:

Uczestnicy szkolenia zyskują praktyczne umiejętności, które można wdrożyć natychmiast – od rozpoznania incydentów po właściwe reagowanie i dokumentowanie. Szkolenie pozwala zrozumieć realne zagrożenia, z jakimi mierzą się JST, w tym phishingowe, ransomware, wycieki danych, etc. Uczestnicy otrzymują konkretne narzędzia i procedury, które pomagają spełnić wymagania prawne i organizacyjne, w tym Krajowy System Cyberbezpieczeństwa. **Szkolenie wzmacnia świadomość pracowników, co realnie obniża ryzyko incydentów** – to najtańsza i najskuteczniejsza forma podniesienia poziomu bezpieczeństwa.

Szkolenie oparte jest na przykładach, scenariuszach i błędach opartych na realnych sytuacjach w JST.

Podczas szkolenia nacisk jest kładziony na ćwiczenia, analizę przypadków, gotowe rozwiązania, które można wdrożyć w urzędzie. **Szkolenie uwzględnia najnowsze ataki na samorządy oraz zmiany legislacyjne, które weszły w 2026 r.**

Podczas szkolenia **nacisk jest położony na: przykłady z życia, praktyczne umiejętności, proste i skuteczne procedury, świadomość i odpowiedzialność oraz minimalizację ryzyka.**

Szkolenie jest istotne z punktu widzenia JST ponieważ: samorządy są jednym z najczęściej atakowanych sektorów, a większość incydentów wynika z błędów ludzkich i braku świadomości; odpowiedzialność za bezpieczeństwo informacji rośnie, a koszt incydentu (utrata danych paraliż usług, odpowiedzialność prawna) jest wielokrotnie wyższy niż koszt szkolenia.

CELE I KORZYŚCI:

- Zbudowanie świadomości realnych zagrożeń cybernetycznych w JST oraz ich wpływu na funkcjonowanie urzędu.
- Wyposażenie uczestników w praktyczne umiejętności rozpoznawania, zapobiegania i zgłaszania incydentów bezpieczeństwa.
- Uporządkowanie wiedzy w zakresie obowiązków prawnych i organizacyjnych związanych z cyberbezpieczeństwem.
- Wzmocnienie kompetencji w obszarze bezpiecznego korzystania z systemów informatycznych, poczty elektronicznej i dokumentów.
- Kształtowanie postawy odpowiedzialności za bezpieczeństwo informacji oraz świadomego ograniczania ryzyka błędów ludzkich.

PROGRAM:

I. BEZPIECZEŃSTWO INFORMACJI

1. **Zakres i znaczenie bezpieczeństwa**
   - Cyberbezpieczeństwo a cyberodporność.
   - Bezpieczeństwo informacji jako element ciągłości działania i przewagi konkurencyjnej.
   - Triada CIA: poufność, integralność, dostępność — jak przekłada się na codzienną pracę.
   - Normy i standardy bezpieczeństwa – powszechnie stosowane rozwiązania.
2. **Rola pracownika i organizacji**
   - Odpowiedzialność indywidualna i zespołowa.

- Najczęstsze błędy ludzkie prowadzące do incydentów.
- Kultura bezpieczeństwa.

II. ZAGROŻENIA CYBERNETYCZNE

3. Ataki zewnętrzne
- Przegląd aktualnych ataków komputerowych.
- Ataki przez sieci bezprzewodowe.
- Ataki przez pocztę e-mail, strony WWW, komunikatory, telefon.
- Ataki APT, phishing, spam, scam, etc.

4. Zagrożenia wewnętrzne
- Nieumyślne błędy pracowników.
- Nadużycia i celowe działania pracowników.
- Shadow IT — prywatne aplikacje i urządzenia w pracy.

5. Zagrożenia fizyczne
- Kradzież lub utrata urządzeń.
- Nieautoryzowany dostęp do pomieszczeń.
- Podsłuchy, niekontrolowane wizyty.

III. INFORMACJE PRAWNIE CHRONIONE W PRZEDSIĘBIORSTWIE

6. Kategorie informacji
- Dane osobowe.
- Tajemnica przedsiębiorstwa.
- Informacje handlowe, finansowe, techniczne.
- Informacje objęte klauzulami poufności.

7. Podstawy prawne:
- Krajowy System Cyberbezpieczeństwa.
- RODO: zasady przetwarzania, obowiązki administratora i pracownika.
- Wewnętrzne polityki bezpieczeństwa, instrukcje zarządzania systemem informatycznym, regulaminy pracy.

IV. BEZPIECZNA PRACA Z SYSTEMAMI I URZĄDZENIAMI

8. Zarządzanie tożsamością i dostępem
- Silne hasła i menedżer haseł.
- MFA (multi-factor authentication) - kiedy jest obowiązkowe, jak działa.
- Zasada najmniejszych uprawnień (reglamentacja dostępu).

9. Bezpieczne korzystanie z poczty i Internetu
- Analiza nagłówków, linków, załączników.
- Rozpoznawanie fałszywych stron logowania.
- Zasady korzystania z przeglądarki, rozszerzeń, VPN.

10. Urządzenia mobilne
- Bezpieczna praca z urządzeniami mobilnymi
- Szyfrowanie dysków i pamięci.
- Zasady korzystania z publicznych sieci Wi Fi.
- Ochrona urządzeń prywatnych wykorzystywanych w pracy (BYOD -
- Bring Your Own Device).

V. OCHRONA DOKUMENTÓW I INFORMACJI W ŚRODOWISKU PRACY

11. Organizacja pracy
- Zasada czystego biurka i czystego ekranu.
- Klasyfikacja informacji i oznaczanie dokumentów.
- Bezpieczne przechowywanie dokumentów papierowych i elektronicznych.

12. Przekazywanie i udostępnianie informacji

- Zasady udostępniania danych wewnątrz i na zewnątrz organizacji.
- Szyfrowanie plików i komunikacji.
- Weryfikacja tożsamości odbiorcy.

13. Brakowanie i archiwizacja

- Niszczarki, procedury utylizacji nośników.

VI. REAGOWANIE NA INCYDENTY BEZPIECZEŃSTWA

14. Rozpoznawanie incydentu

- Nietypowe zachowania systemu.
- Podejrzane wiadomości, etc.

15. Procedury zgłaszania

- Kanały zgłoszeń: IT, IOD, przełożony.
- Jakie informacje przekazać.
- Niezwłoczne zgłoszenie incydentu.

16. Działania po incydencie

- Wsparcie zespołu IT i IOD.
- Analiza przyczyn i wdrażanie środków naprawczych.
- Komunikacja wewnętrzna i zewnętrzna.

VII. ZADANIA KADRY ZARZĄDZAJĄCEJ

17. Zarządzanie ryzykiem

- Identyfikacja, ocena i akceptacja ryzyka.
- Matryce ryzyka i priorytetyzacja działań.

18. Budowanie systemu bezpieczeństwa

- Polityka Bezpieczeństwa Informacji.
- Rola audytów i testów penetracyjnych.
- Zarządzanie dostawcami i bezpieczeństwo łańcucha dostaw.

19. Odpowiedzialność prawna

- Konsekwencje naruszeń RODO.
- Odpowiedzialność zarządu i kierowników.

VIII. AI – SZTUCZNA INTELIGENCJA W SŁUŻBIE OSZUSTÓW (AI HACKING):

20. Phishing i Socjotechnika (Deepfakes).

- Automatyzacja, przyspieszenie i zwiększenie skali działań cyberprzestępczych.

21. Fałszywe tożsamości.

- Wykorzystanie AI do generowania fałszywego wizerunku, obrazu, głosu.

ADRESACI:

Szkolenie skierowane do pracowników, którzy w codziennej pracy korzystają z systemów informatycznych, przetwarzają dane. Szkolenie jest szczególnie wartościowe i niezbędne dla osób, które nie są informatykami, ale ich zachowania i decyzje mają kluczowy wpływ na bezpieczeństwo urzędu.

PROWADZĄCY:

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

Zajmował 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. Jest autorem i współautorem artykułów i publikacji dotyczących bezpieczeństwa informacji. Łączy doświadczenie menedżerskie, audytorskie i szkoleniowe z praktyką operacyjną, co zapewnia wysoki poziom merytoryczny oraz praktyczny charakter prowadzonych szkoleń.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Cyberbezpieczeństwo w JST w praktyce – zapobieganie, reagowanie, zgodność z przepisami

	Szkolenie będziemy realizowali **w formie webinarium online**.
	16 czerwca 2026 r. **Szkolenie w godzinach 09:00-15:00**
	Cena: 479 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

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 ☐

Proszę o przesłanie faktury na adres mailowy: ……

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 poprzez formularz zgłoszenia na www.mistia.org.pl lub mailem na szkolenia@mistia.org.pl do 09 czerwca 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 wystawionej i przesłanej FV.

Podpis osoby upoważnionej _____