Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ONLINE
25 sierpnia 2026

BEZPIECZNY URZĄD W ERZE CYFROWEJ – CYBERZAGROŻENIA, OCHRONA INFORMACJI I ODPOWIEDZIALNOŚĆ PRACOWNIKÓW

WAŻNE INFORMACJE:

Cyberbezpieczeństwo przestało być wyłącznie zagadnieniem technicznym realizowanym przez informatyków. Obecnie jednym z najważniejszych elementów bezpieczeństwa urzędu jest świadomość pracowników oraz ich codzienne decyzje podejmowane podczas korzystania z poczty elektronicznej, systemów informatycznych, Internetu i urządzeń mobilnych.

Jednostki samorządu terytorialnego oraz ich jednostki organizacyjne coraz częściej stają się celem cyberataków. Przestępcy wykorzystują nie tylko luki techniczne, ale przede wszystkim błędy ludzkie, stosując phishing, socjotechnikę, złośliwe oprogramowanie, fałszywe wiadomości e-mail czy próby wyłudzenia danych i środków finansowych. W praktyce nawet pojedyncza nieostrożna czynność pracownika może doprowadzić do poważnego incydentu bezpieczeństwa, utraty danych lub zakłócenia pracy urzędu.

Dodatkową motywacją do podnoszenia kompetencji pracowników są dynamicznie zmieniające się wymagania prawne dotyczące cyberbezpieczeństwa, ochrony danych osobowych oraz bezpieczeństwa informacji. Szczególne znaczenie mają wdrażane w Polsce rozwiązania wynikające z dyrektywy NIS2 oraz planowane zmiany w krajowych regulacjach dotyczących cyberbezpieczeństwa, które zwiększają znaczenie budowania świadomości i odporności organizacji na zagrożenia cyfrowe.

Szkolenie wyróżnia się praktycznym podejściem do tematu. Zamiast skupiać się na technicznych aspektach konfiguracji systemów informatycznych, koncentruje się na rzeczywistych zagrożeniach występujących w codziennej pracy urzędów i jednostek organizacyjnych. Omawiane są autentyczne przykłady incydentów, najczęściej popełniane błędy pracowników oraz sprawdzone metody ograniczania ryzyka.

Szkolenie przeznaczone dla osób początkujących i średniozaawansowanych. Nie wymaga wiedzy informatycznej ani technicznej. Program skierowany jest do pracowników urzędów oraz jednostek organizacyjnych samorządu terytorialnego, którzy na co dzień korzystają z komputerów, poczty elektronicznej i systemów informatycznych.

Uczestnicy otrzymają praktyczne wskazówki dotyczące rozpoznawania zagrożeń, bezpiecznej pracy z informacją, właściwego reagowania na incydenty oraz ochrony danych przetwarzanych w jednostkach sektora publicznego. Zdobyta wiedza będzie mogła zostać wykorzystana bezpośrednio po zakończeniu szkolenia w codziennej pracy zawodowej.

CELE I KORZYŚCI:

Celem szkolenia jest podniesienie poziomu świadomości i kompetencji pracowników jednostek samorządu terytorialnego w zakresie cyberbezpieczeństwa oraz bezpieczeństwa informacji. Uczestnicy poznają najczęściej występujące zagrożenia cybernetyczne, zasady bezpiecznego korzystania z systemów informatycznych i poczty elektronicznej, a także praktyczne metody ochrony danych przetwarzanych w urzędzie i jednostkach organizacyjnych.

Korzyści z udziału w szkoleniu:

- Poznanie najczęściej występujących cyberzagrożeń skierowanych przeciwko urzędom i jednostkom organizacyjnym.
- Zdobycie praktycznych umiejętności rozpoznawania prób phishingu, socjotechniki, fałszywych wiadomości oraz innych metod wykorzystywanych przez cyberprzestępców.
- Nabycie wiedzy dotyczącej bezpiecznego korzystania z poczty elektronicznej, Internetu, urządzeń mobilnych oraz pracy zdalnej.
- Poznanie zasad prawidłowej ochrony informacji, danych osobowych oraz dokumentów elektronicznych w codziennej pracy urzędnika.

- Zwiększenie świadomości odpowiedzialności pracowników za bezpieczeństwo informacji i ciągłość działania urzędu.
- Zdobycie umiejętności właściwego reagowania na incydenty bezpieczeństwa oraz zgłaszania niepokojących zdarzeń.
- Poznanie aktualnych wymagań i obowiązków wynikających z przepisów dotyczących cyberbezpieczeństwa, ochrony danych osobowych oraz bezpieczeństwa informacji w sektorze publicznym.
- Ograniczenie ryzyka wystąpienia incydentów bezpieczeństwa wynikających z błędów ludzkich, które pozostają najczęstszą przyczyną skutecznych cyberataków.
- Poznanie dobrych praktyk budowania kultury bezpieczeństwa w urzędzie oraz jednostkach organizacyjnych.

PROGRAM:

1. **Cyberbezpieczeństwo w administracji publicznej – dlaczego dotyczy każdego pracownika?**
   a. Aktualne zagrożenia dla urzędów i jednostek organizacyjnych.
   b. Najczęstsze przyczyny incydentów bezpieczeństwa.
   c. Konsekwencje utraty danych i zakłócenia pracy urzędu.
   d. Przykłady rzeczywistych incydentów w administracji publicznej.
   e. Rola pracownika w systemie bezpieczeństwa informacji.
2. **Najczęściej spotykane cyberzagrożenia w codziennej pracy urzędu**
   a. Phishing i spear phishing.
   b. Fałszywe wiadomości e-mail i SMS.
   c. Oszustwa związane z podszywaniem się pod przełożonych, kontrahentów i instytucje publiczne.
   d. Ransomware i inne rodzaje złośliwego oprogramowania.
   e. Socjotechnika – manipulacja jako narzędzie cyberprzestępców.
   f. Zagrożenia związane z mediami społecznościowymi.
   g. Analiza przykładowych prób ataków.
3. **Bezpieczna praca z pocztą elektroniczną, Internetem i dokumentami**
   a. Jak rozpoznawać podejrzane wiadomości.
   b. Weryfikacja nadawców i linków.
   c. Bezpieczne pobieranie i otwieranie załączników.
   d. Zasady korzystania z nośników danych.
   e. Udostępnianie dokumentów i plików.
   f. Najczęstsze błędy użytkowników.
   g. Dobre praktyki bezpieczeństwa cyfrowego.
4. **Ochrona informacji i danych osobowych w codziennej pracy**
   a. Informacja jako zasób urzędu.
   b. Ochrona danych osobowych a cyberbezpieczeństwo.
   c. Bezpieczne przetwarzanie dokumentów elektronicznych i papierowych.
   d. Czyste biurko i czysty ekran.
   e. Praca zdalna i mobilna – zagrożenia oraz dobre praktyki.
   f. Bezpieczeństwo urządzeń mobilnych.
5. **Hasła, uwierzytelnianie i bezpieczny dostęp do systemów**
   a. Dlaczego hasła nadal są jednym z najważniejszych elementów bezpieczeństwa.
   b. Najczęściej popełniane błędy przy tworzeniu haseł.
   c. Menedżery haseł – korzyści i zagrożenia.
   d. Uwierzytelnianie wieloskładnikowe (MFA).
   e. Bezpieczne korzystanie z kont służbowych.
6. **Jak reagować na incydenty bezpieczeństwa?**
   a. Jak rozpoznać incydent bezpieczeństwa.
   b. Pierwsze działania po wykryciu zagrożenia.
   c. Zasady zgłaszania incydentów.
   d. Czego nie robić po wystąpieniu incydentu.
   e. Współpraca z administratorami i osobami odpowiedzialnymi za bezpieczeństwo.
7. **Aktualne obowiązki jednostek sektora publicznego i kierunki zmian w przepisach**
   a. Podstawowe regulacje dotyczące cyberbezpieczeństwa.
   b. Dyrektywa NIS2 i jej znaczenie dla sektora publicznego.
   c. Krajowy System Cyberbezpieczeństwa.
   d. Odpowiedzialność pracowników i kierownictwa za bezpieczeństwo informacji.

e. Budowanie kultury cyberbezpieczeństwa w organizacji.

8. **Podsumowanie szkolenia, pytania uczestników i omówienie najważniejszych rekomendacji**
   a. Najważniejsze zasady bezpiecznej pracy.
   b. Lista dobrych praktyk do wdrożenia po szkoleniu.
   c. Odpowiedzi na pytania uczestników.
   d. Dyskusja i wymiana doświadczeń.

ADRESACI:

Szkolenie skierowane jest przede wszystkim do pracowników jednostek samorządu terytorialnego oraz jednostek organizacyjnych sektora publicznego, którzy w codziennej pracy korzystają z komputerów, poczty elektronicznej, systemów informatycznych oraz przetwarzają informacje i dane.

W szczególności udział w szkoleniu rekomendowany jest dla:

- pracowników urzędów gmin, miast, starostw powiatowych oraz urzędów marszałkowskich,
- kierowników wydziałów, referatów i jednostek organizacyjnych,
- pracowników sekretariatów i biur obsługi klienta,
- pracowników wydziałów organizacyjnych, administracyjnych i kancelaryjnych,
- pracowników wydziałów finansowych, budżetowych i księgowości,
- pracowników kadr i płac,
- pracowników zajmujących się ochroną danych osobowych i bezpieczeństwem informacji,
- pracowników jednostek organizacyjnych JST, takich jak szkoły, przedszkola, centra usług wspólnych, ośrodki pomocy społecznej, centra usług społecznych, domy kultury, biblioteki, jednostki sportu i rekreacji oraz inne jednostki samorządowe,
- osób odpowiedzialnych za obieg dokumentów, kontakt z mieszkańcami oraz realizację spraw administracyjnych.

*Uwaga! Szkolenie nie jest przeznaczone dla administratorów systemów informatycznych, specjalistów ds. cyberbezpieczeństwa, informatyków zajmujących się konfiguracją i utrzymaniem infrastruktury teleinformatycznej oraz osób oczekujących zaawansowanej wiedzy technicznej dotyczącej zabezpieczania sieci, serwerów i systemów informatycznych.

PROWADZĄCY:

trener specjalizujący się w obszarze kompetencji cyfrowych, cyberbezpieczeństwa, sztucznej inteligencji oraz praktycznego wykorzystania nowoczesnych technologii w administracji publicznej, edukacji i biznesie. Posiada ponad 15 lat doświadczenia w prowadzeniu szkoleń oraz warsztatów dla jednostek samorządu terytorialnego, administracji publicznej, instytucji edukacyjnych, uczelni wyższych, organizacji pozarządowych oraz przedsiębiorstw. Przeprowadził ponad 22 000 godzin szkoleń obejmujących m.in. cyberbezpieczeństwo, ochronę danych, sztuczną inteligencję, pakiet Microsoft 365, analizę danych, automatyzację procesów oraz kompetencje cyfrowe.

W swojej pracy łączy wiedzę techniczną z praktyką funkcjonowania urzędów i jednostek organizacyjnych. Prowadzi szkolenia koncentrujące się na rzeczywistych zagrożeniach, najczęściej popełnianych błędach użytkowników oraz skutecznych metodach ograniczania ryzyka wystąpienia incydentów bezpieczeństwa informacji. Realizował projekty szkoleniowe dla administracji samorządowej, jednostek pomocy społecznej, placówek oświatowych, instytucji kultury, uczelni oraz przedsiębiorstw. Szczególną uwagę poświęca praktycznym aspektom cyberbezpieczeństwa, ochrony danych osobowych, bezpiecznej pracy z informacją oraz budowaniu świadomości zagrożeń wśród pracowników.

Autor programów szkoleniowych i materiałów dydaktycznych wykorzystywanych podczas szkoleń dla administracji publicznej i sektora edukacji. Regularnie prowadzi szkolenia z zakresu cyberbezpieczeństwa, ochrony danych, sztucznej inteligencji oraz bezpiecznego korzystania z technologii cyfrowych.

Prowadzone przez niego szkolenia cenione są za praktyczne podejście, wykorzystanie rzeczywistych przykładów oraz dostosowanie omawianych zagadnień do specyfiki pracy uczestników.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Bezpieczny urząd w erze cyfrowej – cyberzagrożenia, ochrona informacji i odpowiedzialność pracowników

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

25 sierpnia 2026 r. **Szkolenie w godzinach 9.00-13.30**

Cena: 479 zł netto/os. Zgłaszając się do 6 sierpnia obowiązuje promocyjna cena 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 poprzez formularz zgłoszenia na www.mistia.org.pl do 20 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 _____