Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
22 czerwca 2023 r.

CO KAŻDY KIEROWNIK WIEDZIEĆ POWINIEN O CYBERBEZPIECZEŃSTWIE? CZYLI PRAKTYCZNE WSKAZÓWKI DLA KADRY ZARZĄDZAJĄCEJ JST

WAŻNE INFORMACJE:

Proponowane szkolenie z zakresu cyberbezpieczeństwa dedykujemy kadrze zarządzającej. Podczas zajęć krok po kroku przeanalizujemy podstawy cyberbezpieczeństwa i bezpieczeństwa Informacji oraz rolę zarządzających jednostką w tych procesach. Przedmiotem zajęć jest:

- Przedstawienie sposobów skutecznego zwiększania świadomości cyberzagrożeń wśród pracowników.
- Poznanie najczęstszych błędów popełnianych przez urzędy w zakresie cyberbezpieczeństwa, które „widać" podczas testów i audytów.
- Uświadomienie, że przestępcy mogą się podszyć pod każdy numer telefonu, e-mail i stronę www.
- Poznanie skutecznych metod unikania ataków phishingowych – praktyczne przykłady.
- Wskazanie co powinno się zrobić jeśli dojdzie do ataku.
- Zapoznanie się z rzeczywistymi konsekwencjami cyberataków dla JST np. ataku typu ransomware.
- Poznanie narzędzi, dzięki którym każdy użytkownik może sprawdzić czy otrzymany link lub załącznik w e-mailu jest niebezpieczny.

CELE I KORZYŚCI:

- Omówienie zagadnień związanych z cyberbezpieczeństwem i ochroną informacji (w tym danych osobowych) w jednostkach publicznych w kontekście istotnej roli kadry zarządzającej w całym procesie.
- Przedstawienie zasad „cyberhigieny", które pomogą dyrektorom/kierownikom sprawniej zarządzać swoimi komórkami organizacyjnymi.
- Omówienie przykładowych ataków oraz kradzieży i wycieków danych z jst oraz konsekwencji dla instytucji.
- Wskazanie dobrych praktyk minimalizowania konsekwencji cyberataku.
- Omówienia przykładowych działań zmniejszających koszty zapewnienia cyberbezpieczeństwa.

PROGRAM:

1. Rola kadry zarządzającej w procesie ochrony informacji i zapewnienia cyberbezpieczeństwa.
2. Przegląd aktów prawnych dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa: RODO, KRI, KSC.
3. Budowa kultury ochrony informacji jako wyzwanie dla każdej organizacji. Dlaczego jest tak ważne?
4. Sposoby skutecznego zwiększania świadomości cyberzagrożeń wśród pracowników.
5. Przykładowe ataki, kradzieże i wycieki danych w JST.
6. Zasady „cyberhigieny". Czyli jak wspomóc dyrektora/kierownika w bezpiecznym zarządzaniu zespołem?
7. Jakie są konsekwencje incydentu? Jakie są najczęstsze incydenty? Czy każdy incydent trzeba zgłaszać?
8. Phishing i ransomware. Aktualnie największe zagrożenie dla każdej organizacji.
9. Przykłady podszywania się cyberprzestępców pod kontrahentów, pracowników lub instytucje: telefon, mail, strona www, komunikatory.
10. Metody unikania ataków phishingowych?
11. Dlaczego ransomware jest tak groźny?
12. Proste narzędzia pomagające każdemu pracownikowi sprawdzić czy otrzymany link lub załącznik w e-mailu jest niebezpieczny. Przykłady. A co zrobić, gdy już coś „się jednak kliknęło"?
13. Testy i audyty bezpieczeństwa. Korzyści dla JST.
14. Najczęstsze błędy popełniane przez urzędy w zakresie cyberbezpieczeństwa, które „widać" podczas testów i audytów.
15. Podsumowanie. Pytania i odpowiedzi.

ADRESACI:

Kadra zarządzająca jednostkami administracji publicznej (sekretarze, dyrektorzy, kierownicy), osoby koordynujące i nadzorujące pracę audytorów wewnętrznych, osoby koordynujące i nadzorujące pracę zespołów IT.

PROWADZĄCY:

Audytor, trener, doradca. Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń. Audytor wiodący normy ISO/IEC 27001:2017. Członek Polskiego Towarzystwa Informatycznego. Prowadzi audyty bezpieczeństwa oraz szkolenia i konsultacje m.in. z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa oraz budowania kultury ochrony informacji.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Co każdy kierownik wiedzieć powinien o cyberbezpieczeństwie? Czyli praktyczne wskazówki dla kadry zarządzającej JST

	Szkolenie będziemy realizowali **w formie webinarium on line**.
	22 czerwca 2023 r. **Szkolenie w godzinach 10:00-14:00**
	Cena: 395 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:	FRDL Małopolski Instytut Samorządu Terytorialnego i Administracji 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 16 czerwca 2023 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 _____