Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
29 stycznia 2024 r.

WPROWADZENIE DO AUDYTÓW BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA W JST

INFORMACJE O SZKOLENIU:

Cyberprzestępcy coraz częściej biorą na cel jednostki administracji publicznej a ewentualne kradzieże lub wycieki danych z jst mogą mieć duże konsekwencje dla samych jednostek (np. kary finansowe) oraz mieszkańców gminy lub powiatu. Pracownicy i kadra zarządzająca jst wykorzystują wdrożone polityki, procedury i instrukcje bezpieczeństwa, liczne zabezpieczenia fizyczne a działy IT wdrażają rozwiązania techniczne, aby chronić przetwarzane dane. **Ale czy te 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? Czy znają procedury? Czy w ogóle takie procedury są wdrożone? Czy wewnętrzne polityki i procedury oraz same systemy IT są aktualizowane, aby odpowiadały bieżącym wymaganiom i przeciwstawiały się realnym zagrożeniom? Audyt odpowiada m.in. na te pytania i jest obiektywną formą weryfikacji, sprawdzenia na ile nasze zabezpieczenia działają. Konieczność audytowania jst w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa wynika z przepisów (RODO, KRI, KSC) oraz dobrych praktyk, ponieważ nie ma lepszej drogi do sprawdzenia czy nasze zabezpieczenia i procedury działają jak ich weryfikacja.

Odpowiedzią na powyższe rozważania jest proponowane przez nas szkolenie, podczas którego krok po kroku:

- omówimy przydatne narzędzia w zapewnieniu skutecznego przeprowadzenia audytu bezpieczeństwa;
- przeanalizujemy praktyczne aspekty prowadzenia audytu oraz bycia audytowanym;
- wyjaśnimy na czym polegają najczęstsze błędy popełniane przez jst w zakresie cyberbezpieczeństwa, które „widać" i „słychać" podczas audytów;
- pokażemy na przykładach jak przeprowadzić audyt wewnętrzny.

CELE I KORZYŚCI:

- Zdobędziesz, uzupełnisz i uporządkujesz wiedzę związaną z ochroną informacji (w tym danych osobowych) oraz cyberbezpieczeństwem w jednostkach publicznych w kontekście prowadzenia audytów (wewnętrznych i zewnętrznych).
- Poznasz zasady przygotowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
- Dowiesz się jakie są podstawowe zasady przygotowania i prowadzenia audytów bezpieczeństwa.
- Poznasz dobre praktyki dotyczących audytów KRI.
- Zapoznasz się z praktycznymi zasadami dotyczącymi analizy ryzyka w bezpieczeństwie informacji.
- Dowiesz się jakie są najczęściej popełniane błędy i nieprawidłowości w zakresie bezpieczeństwa przetwarzania informacji i cyberbezpieczeństwa w jednostkach oraz poznasz sposoby postępowania mające na celu ich eliminację.
- Uzyskasz odpowiedzi na pojawiające się pytania i wątpliwości związane z przedmiotem zajęć.

PROGRAM:

1. Przegląd aktów prawnych dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa: RODO, KRI, KSC.
2. Dyrektywa NIS2 – nowe obowiązki dla podmiotów publicznych.
3. Budowa kultury ochrony informacji jako wyzwanie dla każdej organizacji - szanse i zagrożenia.
4. System Zarządzania Bezpieczeństwem Informacji (SZBI) Jak zbudować? Od czego zacząć?
5. Przegląd norm serii ISO 27xxx.
6. Testy i audyty bezpieczeństwa – rodzaje i korzyści.
7. Przygotowanie audytora / Komunikacja podczas audytów / Predyspozycje audytora.
8. Audyty KRI – założenia, główne obszary, przebieg, dobre praktyki, wnioski.
9. Jak samodzielnie przeprowadzić audyt bezpieczeństwa?
10. Przegląd przykładowych działań korygujących i doskonalących po audytach KRI.
11. Analiza ryzyka w bezpieczeństwie informacji. Przykłady.
12. Zasoby, podatności i zagrożenia – sposoby identyfikacji na potrzeby szacowania ryzyka.
13. Podsumowanie. Dyskusja.

ADRESACI:

Osoby koordynujące i nadzorujące pracę audytorów wewnętrznych, osoby koordynujące i nadzorujące pracę zespołów IT, pracownicy komórek audytu i kontroli, zespoły IT, Inspektorzy Ochrony Danych.

PROWADZĄCY:

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

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Wprowadzenie do audytów bezpieczeństwa informacji i cyberbezpieczeństwa w JST

	Szkolenie będziemy realizowali **w formie webinarium on line**.
	29 stycznia 2024 r. **Szkolenie w godzinach 10:00-14:00**
	Cena: 435 PLN netto/os. Przy zgłoszeniu do 15 stycznia 2024 r. cena wynosi 399 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 Podlaskie Centrum ul. Wrocławska 51, 15-644 Białystok tel.: 85 732 17 88 | fax: 85 732 94 84 mail: frdl-pc@frdl.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.frdl.bialystok.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na frdl-pc@frdl.org.pl do 23 stycznia 2024 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 _____