Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

KURS ON-LINE:
29, 30, 31 marca 2023 r.

KURS: OCHRONA INFORMACJI NIEJAWNYCH W INSTYTUCJI.

DOKUMENTOWANIE I PRZETWARZANIE INFORMACJI NIEJAWNYCH ORAZ STOSOWANIE ŚRODKÓW BEZPIECZEŃSTWA W JEDNOSTCE. NIEZBĘDNE PROCEDURY I PRAKTYKA

CELE I KORZYŚCI

Uczestnicy 3-dniowego kursu, w jego trakcie:

- Zdobędą wiedzę i nabędą praktyczne umiejętności w zakresie zastosowania wymagań, które są określone w ustawie o ochronie informacji niejawnych, a które będą mogli wprowadzić ich w życie w jednostce czy instytucji na przykładzie konkretnych rozwiązań, wzorów oraz wskazówek, pochodzących z wieloletniej praktyki eksperta, wynikającej z jego wykształcenia i doświadczenia zawodowego.
- Poznają rolę i zadania, jakie mają kierownik jednostki i pełnomocnik ds. ochrony informacji niejawnych.
- Zapoznają się z obowiązkami informacyjnymi kierownika jednostki oraz pełnomocnika ochrony, zasadami współpracy, podziału zadań oraz kwestii odpowiedzialności.
- Nabędą umiejętności w zakresie opracowania i wdrożenia w jednostce niezbędnej dokumentacji z zakresu OIN, wymaganej ustawą.
- Dowiedzą się jak właściwie zorganizować obieg materiałów niejawnych na poziomie klauzuli „poufne" i „zastrzeżone", jak klasyfikować informacje niejawne oraz jak rejestrować ich obieg w dziennikach i urządzeniach kancelaryjnych, a także jakie zasady ochrony informacji niejawnych, w tym reguły związane ze stosowaniem przepisów o RODO, stosować w celu prawidłowego funkcjonowania systemu w jednostce/ instytucji.
- Poznają tematykę kontroli prowadzonych przez ABW.
- Poddadzą analizie problematykę akredytacji systemów teleinformatycznych, które służą do przetwarzania informacji niejawnych, czy prowadzenia dokumentacji bezpieczeństwa teleinformatycznego.
- Będą mieli możliwość konsultacji, podczas 3 dni zajęć, kwestii problemowych z ekspertem - praktykiem.
- Kurs zakończymy testem sprawdzającym wiedzę.

WAŻNE INFORMACJE O KURSIE:

Udział w 3 – dniowym kursie gwarantuje zdobycie i usystematyzowanie wiedzy z zakresu ochrony informacji niejawnych, bezpieczeństwa teleinformatycznego w jednostce, zarządzania ryzykiem w zakresie OIN.

Jest doskonałą okazją do poznania tej skomplikowanej materii, w szczególności jej praktycznych aspektów.

Podczas zajęć ekspert wskaże problemy związane z właściwą organizacją pracy kancelarii materiałów niejawnych, ewidencja dokumentów oraz zasadami ich przechowywania czy archiwizacji.

Jakie zadania i obowiązki ma kierownik jednostki organizacyjnej, a jakie pełnomocnik ds. OIN?
Jak właściwie opracować dokumentację wymaganą ustawą o ochronie informacji niejawnych?
Jak należy rejestrować obieg dokumentów niejawnych w dziennikach i urządzeniach kancelaryjnych?
Jak klasyfikować informacje niejawne?
Jak archiwizować i brakować materiały niejawne?
Jak właściwie dokumentować bezpieczeństwo teleinformatyczne?
To tylko niektóre z pytań, na które odpowiemy podczas zajęć.

Ekspert prowadzący zajęcia to menedżer bezpieczeństwa informacji, osoba z dużym doświadczeniem, praktyk w zakresie prowadzenia, tworzenia i nadzoru nad dokumentacją wytwarzaną i przechowywaną w jednostce w zgodnie z RODO i OIN. Posiada również olbrzymią wiedzę i umiejętności w tematyce zarządzania bezpieczeństwem informacji, które potrafi przekazać w prosty i zwięzły sposób.

PROGRAM SZKOLENIA

DZIEŃ I. 29 marca

PODSTAWY OCHRONY INFORMACJI NIEJAWNYCH:

1. **Tajemnice prawnie chronione w Polsce.**
2. **Aktualne podstawy prawne ochrony informacji niejawnych - przepisy ogólne i resortowe.**
3. **Podstawowe zasady ochrony informacji niejawnych.**
4. **Nadzór nad systemem ochrony informacji niejawnych w Polsce:**
   - Kolegium ds. Służb Specjalnych,
   - Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego.
5. **Ochrona informacji niejawnych w jednostkach organizacyjnych: kierownik jednostki organizacyjnej i pełnomocnik ds. ochrony informacji niejawnych (podział ról i zadań).**
6. **Pion ochrony w jednostce organizacyjnej – struktura i wymagania wobec personelu.**
7. **Dokumentacja ochrony informacji niejawnych:**
   - ocena poziomu zagrożeń,
   - instrukcja dotyczącą sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone" oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony,
   - instrukcja przetwarzania informacji niejawnych o klauzuli „poufne",
   - plan ochrony informacji niejawnych,
   - dokumentacja pełnomocnika ochrony,
   - szkolenia z zakresu ochrony informacji niejawnych - terminy, częstotliwość, dokumentacja, ewidencje.
8. **Bezpieczeństwo osobowe – zasady dostępu do informacji niejawnych:**
   - klauzula „zastrzeżone" – upoważnienia,
   - klauzula „poufne" - postępowania sprawdzające (zwykłe i poszerzone),
   - informacje międzynarodowe,
   - teczki akt postepowań sprawdzających – zawartość, przechowywanie i udostępnianie.
9. **Obowiązki informacyjne kierownika jednostki organizacyjnej i pełnomocnika ochrony.**
10. **Karty informacyjne – zasady przesyłania ich do ABW.**

Dzień II. 30 marca

ZAGADNIENIA ZWIĄZANE Z PRZETWARZANIEM INFORMACJI NIEJAWNYCH I STOSOWANIEM ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO W CELU ICH OCHRONY W PRAKTYCE. BEZPIECZEŃSTWO PRZEMYSŁOWE:

1. **Ochrona informacji niejawnych w stosunkach międzynarodowych. Krajowa Władza Bezpieczeństwa.**
2. **System kancelarii tajnych oraz kancelarii tajnych międzynarodowych.**
3. **Organizacja obiegu materiałów niejawnych na poziomie klauzuli „poufne" i „zastrzeżone".**
4. **Zasady rejestracji oraz prowadzenia ewidencji i urządzeń kancelaryjnych.**
5. **Jak należy rejestrować obieg dokumentów niejawnych w dziennikach i urządzeniach kancelaryjnych?**
6. **Jak klasyfikować informacje niejawne? Jakie są okresy ochronne?**
7. **Jak archiwizować i brakować materiały niejawne?**
8. **Zasady punktacji środków bezpieczeństwa fizycznego. Normy, mające zastosowanie przy ochronie informacji niejawnych.**
9. **Omówienie typowych środków bezpieczeństwa, stosowanych w celu ochrony informacji niejawnych:**
   - strefy ochronne,
   - szafy metalowe i meble biurowe,
   - pomieszczenia oraz zamki, ściany i stropy, drzwi i okna,
   - budynki,
   - system kontroli dostępu,
   - personel bezpieczeństwa (pion ochrony, firma ochroniarska),

- system sygnalizacji włamania i napadu,
- monitoring wizyjny,
- ogrodzenie i oświetlenie terenu.

10. **Certyfikacja środków bezpieczeństwa fizycznego.**
11. **Zasady dostępu do informacji niejawnych przez przedsiębiorców.**
12. **Kwestionariusz bezpieczeństwa przemysłowego.**
13. **Świadectwa bezpieczeństwa przemysłowego – rodzaje i terminy ważności.**
14. **Podstawowe wymagania związane z zawieraniem z przedsiębiorcami umów, których realizacja wiąże się z dostępem do informacji niejawnych.**
15. **RODO a ochrona informacji niejawnych.**
16. **Informacje niejawne a prawo dostępu do informacji publicznej.**

Dzień III. 31 marca

BEZPIECZEŃSTWO TELEINFORMATYCZNE. JAK PRAWIDŁOWO JE REALIZOWAĆ W JEDNOSTCE?

1. **Przetwarzanie informacji niejawnych w systemach i sieciach teleinformatycznych. Zasady ogólne.**
2. **Personel bezpieczeństwa**:
   - Administrator Systemu i Inspektor Bezpieczeństwa Teleinformatycznego,
   - wymagania formalne, rola i zadania.
3. **Akredytacja systemów teleinformatycznych, służących do przetwarzania informacji niejawnych.**
4. **Dokumentacja bezpieczeństwa teleinformatycznego:**
   - szczególne Wymagania Bezpieczeństwa Systemu,
   - procedury Bezpiecznej Eksploatacji.
5. **Analiza ryzyka oraz zarzadzanie ryzykiem związanym z przetwarzaniem informacji niejawnych.**
6. **Kryptografia i środki ochrony elektromagnetycznej.**
7. **Środki bezpieczeństwa fizycznego stosowane w celu ochrony systemów i sieci przetwarzających informacje niejawne.**
8. **Sprzętowa Strefa Ochrony Elektromagnetycznej.**
9. **Procedury kontrolne w bezpieczeństwie teleinformatycznym.**
10. **Podstawy konfiguracji BIOS i systemu operacyjnego Microsoft Windows 10 Professional w systemie teleinformatycznym, przetwarzającym informacje niejawne.**
11. **Brakowanie nośników informatycznych służących do przetwarzania materiałów niejawnych.**

KURS zakończy się testem, sprawdzającym wiedzę!

ADRESACI

kierownicy jednostek, sekretarze w jednostkach samorządu terytorialnego, pełnomocnicy ds. ochrony informacji niejawnych, osoby odpowiedzialne za rejestrację i obieg dokumentów niejawnych/ kierownicy Kancelarii Materiałów Niejawnych, pracownicy komórek zarządzania kryzysowego i OC, pracownicy komórek organizacyjnych odpowiedzialnych w jednostce za ochronę informacji niejawnych.

PROWADZĄCY

Absolwent UMK w Toruniu oraz studiów podyplomowych WSAiB w Gdyni na kierunku zarządzanie bezpieczeństwem informacji, certyfikowany Inspektor Ochrony Danych, Menedżer Bezpieczeństwa Informacji oraz Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji. W latach 1992 - 2013 funkcjonariusz UOP/ABW, od 1999 r. zajmuje się problematyką ochrony informacji niejawnych i innych danych prawnie chronionych, od 2009 r. ekspert ABW z zakresu OIN. Współorganizator szkoleń i konferencji poświęconych problematyce ochrony informacji oraz danych osobowych. W latach 2013 - 2017 Pełnomocnik ds. ochrony informacji niejawnych w Urzędzie Wojewódzkim oraz innych jednostkach.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

NFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Kurs: Ochrona informacji niejawnych w instytucji. Dokumentowanie i przetwarzanie informacji niejawnych oraz stosowanie środków bezpieczeństwa w jednostce. Niezbędne procedury i praktyka

	Kurs będziemy realizowali **w formie webinarium on line**.
	**29, 30, 31 marca 2023 r.** **Kurs każdego dnia w godzinach 9:30-14:00**
	**Cena: 859 zł netto/os. przy zgłoszeniu 28 lutego, Cena 920 PLN netto/os. przy zgłoszeniu od 1 marca.** Udział w kursie zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.
CENA zawiera:	udział w profesjonalnym kursie online z możliwości zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.
Dane do kontaktu:	Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego ul. Żurawia 43, 00-680 Warszawa tel. 17 862 69 64 post@frdl.rzeszow.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.org.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.org.pl do 23 marca 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 _____