Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

KURS ON-LINE:
16, 22, 23 lutego 2024 r.

KURS: OCHRONA INFORMACJI NIEJAWNYCH W JEDNOSTKACH: PAŃSTWOWYCH, SAMORZĄDOWYCH I PRYWATNYCH.

PRZETWARZANIE INFORMACJI NIEJAWNYCH I STOSOWANIE ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO. BEZPIECZEŃSTWO TELEINFORMATYCZNE. PROCEDURY I PRAKTYKA

CELE I KORZYŚCI

- Podniesienie wiedzy i praktycznych umiejętności uczestników dotyczących zastosowania wymagań, które są określone w ustawie o ochronie informacji niejawnych i wprowadzenia ich w życie w administracji publicznej, w szczególności w jst na przykładzie konkretnych rozwiązań, przykładów i wzorów, także pochodzących z wieloletniej praktyki eksperta, wynikającej z jego wykształcenia i doświadczenia zawodowego.
- Nabycie/udoskonalenie przez uczestników **umiejętności opracowania niezbędnej dokumentacji, wymaganej ustawą o ochronie informacji niejawnych.**
- Prezentacja praktycznych zagadnień związanych **z przetwarzaniem informacji niejawnych i stosowaniem środków bezpieczeństwa fizycznego w celu ich ochrony, a także bezpieczeństwa przemysłowego,** tak, aby skutecznie móc zabezpieczyć posiadane informacje niejawne, racjonalnie gospodarując przy tym środkami finansowymi.
- Przedstawienie, krok po kroku obowiązujących zasad **ochrony informacji niejawnych, w tym zasad powiązanych z RODO, niezbędnych do prawidłowego funkcjonowania systemu w jednostce/ instytucji.**
- Analiza problematyki **akredytacji systemów teleinformatycznych,** które służącą do przetwarzania informacji niejawnych, prowadzenia dokumentacji bezpieczeństwa teleinformatycznego.
- Omówienie **szczegółowej analizy ryzyka oraz zarządzania ryzykiem** w zakresie przetwarzania informacji niejawnych, procedur kontrolnych w bezpieczeństwie teleinformatycznym**.**
- **Weryfikacja własnych umiejętności dotyczących praktycznego stosowania przepisów, w celu wyeliminowania błędów i nieprawidłowości w bieżącej pracy.**
- Możliwość konsultacji kwestii problemowych z ekspertem, praktykiem oraz z innymi uczestnikami.

KURS zakończy się egzaminem, sprawdzającym wiedzę!

WAŻNE INFORMACJE O KURSIE:

Podczas kursu ekspert w sposób jasny i przejrzysty omówi kwestie związane z właściwą organizacją pracy kancelarii materiałów niejawnych, ewidencji dokumentów oraz zasad przechowywania i archiwizacji.

Ponadto zostanie przeanalizowana problematyka kontroli prowadzonych przez ABW. Omówimy obowiązki informacyjne kierownika jednostki oraz pełnomocnika ochrony, zasady współpracy, podziału zadań.

Udział w kursie gwarantuje zdobycie i usystematyzowanie kompleksowej wiedzy oraz z zakresu ochrony informacji niejawnych, bezpieczeństwa teleinformatycznego w jednostce, zarządzania ryzykiem w zakresie OIN. Jest doskonałą okazją do poznania tej zawiłej materii, zarówno od strony teoretycznej, jak i praktycznej.

Ekspert prowadzący zajęcia to osoba z dużym doświadczeniem praktycznym w zakresie prowadzenia, tworzenia i nadzoru nad polityką ochrony danych osobowych, RODO i OIN w jednostce/ instytucji.

PROGRAM SZKOLENIA

DZIEŃ I 16 lutego 2024 r.

PODSTAWY OCHRONY INFORMACJI NIEJAWNYCH

1. Tajemnice prawnie chronione w Polsce.
2. Podstawy prawne ochrony informacji niejawnych - przepisy ogólne i resortowe.
3. Elementarne zasady ochrony informacji niejawnych.
4. Systemem ochrony informacji niejawnych w Polsce i nadzór nad nim:
   - Kolegium ds. Służb Specjalnych.
   - Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego.
5. Ochrona informacji niejawnych w jednostkach organizacyjnych – rola i zadania kierownik jednostki organizacyjnej oraz pełnomocnik ds. ochrony informacji niejawnych.
6. Pion ochrony w jednostce organizacyjnej – zadania, struktura i wymagania wobec personelu.
7. Wymagana 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, dokumentowanie szkoleń, prowadzone ewidencje.
8. Bezpieczeństwo osobowe – zasady dostępu do informacji niejawnych.
   - Klauzula „Zastrzeżone" – upoważnienia.
   - Klauzula „Poufne" - postępowania sprawdzające (zwykłe i poszerzone).
9. Informacje niejawne międzynarodowe.
10. Teczki akt postępowań sprawdzających – zawartość, przechowywanie i udostępnianie.
11. Obowiązki informacyjne Kierownika Jednostki Organizacyjnej i Pełnomocnika Ochrony. Karty informacyjne – zasady przesyłania ich do ABW.

DZIEŃ II 22 lutego 2024 r.

PRAKTYCZNE ZAGADNIENIA ZWIĄZANE Z PRZETWARZANIEM INFORMACJI NIEJAWNYCH I STOSOWANIEM ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO W CELU ICH OCHRONY. 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. Zakładanie, rejestracja oraz prowadzenie ewidencji i urządzeń kancelaryjnych.
5. Dokumentowanie obiegu dokumentów niejawnych w dziennikach i urządzeniach kancelaryjnych.
6. Zasady klasyfikowanie informacji niejawnych i oznaczania klauzulami tajności. Okresy ochronne w przeszłości i obecnie.
7. Archiwizacja i brakowanie materiałów niejawnych.
8. Stosowanie środków bezpieczeństwa fizycznego oraz ich punktacja. Normy mające zastosowanie przy ochronie informacji niejawnych.
9. Omówienie typowych środków bezpieczeństwa wykorzystywanych do ochrony informacji niejawnych:
   - Strefy ochronne.
   - Szafy metalowe i meble biurowe.
   - Pomieszczenia oraz zamki, ściany i stropy, drzwi i okna.
   - Budynki.
   - Systemy 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 23 lutego 2024 r.

BEZPIECZEŃSTWO TELEINFORMATYCZNE

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.

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 1999r. zajmuje się problematyką ochrony informacji niejawnych i innych danych prawnie chronionych, od 2009r. 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

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Kurs: Ochrona informacji niejawnych w jednostkach: państwowych, samorządowych i prywatnych. Przetwarzanie informacji niejawnych i stosowanie środków bezpieczeństwa fizycznego. Bezpieczeństwo teleinformatyczne. Procedury i praktyka

Kurs będziemy realizowali **w formie webinarium on line**.

16, 22, 23 lutego 2024 r. **Kurs każdego dnia w godzinach 9:00-13:00**

Cena: 995 zł netto/os. Przy zgłoszeniu do **2 lutego 2024 r. cena 915 zł netto/os.** 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 Centrum Mazowsze;
ul. Jelinka 6, 01-646 Warszawa;
tel. 535 162 759;
szkolenia@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.mazowsze.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Zgłoszenia prosimy przesyłać do 13 lutego 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 _____