

KURS: OCHRONA INFORMACJI NIEJAWNYCH W INSTYTUCJI. PRZETWARZANIE INFORMACJI NIEJAWNYCH, BEZPIECZEŃSTWO TELEINFORMATYCZNE. NIEZBĘDNE PROCEDURY I PRAKTYKA



CELE I KORZYŚCI

Uczestnictwo w 3 dniowym kursie dostarczy Państwu kompleksową wiedzę i pozwoli nabyć praktyczne umiejętności dotyczące ochrony informacji niejawnych, w tym bezpieczeństwa teleinformatycznego w jednostce/ instytucji.

- Podniesienie wiedzy i praktycznych umiejętności uczestników w zakresie 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 służą 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.
- Możliwość konsultacji kwestii problemowych z ekspertem, praktykiem oraz z innymi uczestnikami.

WAŻNE INFORMACJE O SZKOLENIU:

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 zawitej 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.



DZIEŃ I. 31 maja

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 dotycząca 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.
- 8. Szkolenia z zakresu ochrony informacji niejawnych.**
- 9. Bezpieczeństwo osobowe – zasady dostępu do informacji niejawnych:**
 - upoważnienia do klauzuli „Zastrzeżone”,
 - postępowania sprawdzające - zwykłe i poszerzone,
 - teczki akt postępowania sprawdzających – zawartość, przechowywanie i udostępnianie.
- 10. Obowiązki informacyjne Kierownika Jednostki Organizacyjnej i Pełnomocnika Ochrony. Karty informacyjne.**

Dzień II. 1 czerwca

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. Zasady prowadzenia ewidencji i urządzeń kancelaryjnych.**
- 5. Klasyfikowanie informacji niejawnych. Okresy ochronne.**
- 6. Archiwizacja i brakowanie materiałów niejawnych.**
- 7. Zasady punktacji środków bezpieczeństwa fizycznego. Normy mające zastosowanie przy ochronie informacji niejawnych.**
- 8. Omówienie typowych środków bezpieczeństwa stosowanych do 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.
9. **Certyfikacja środków bezpieczeństwa fizycznego.**
 10. **Zasady dostępu do informacji niejawnych przez przedsiębiorców.**
 11. **Kwestionariusz bezpieczeństwa przemysłowego.**
 12. **Świadectwa bezpieczeństwa przemysłowego – rodzaje i terminy ważności.**
 13. **Podstawowe wymagania związane z zawieraniem z przedsiębiorcami umów, których realizacja wiąże się z dostępem do informacji niejawnych.**
 14. **RODO a ochrona informacji niejawnych.**
 15. **Informacje niejawne a prawo dostępu do informacji publicznej.**
 16. **Informacje niejawne a ochrona danych osobowych.**

Dzień III. 2 czerwca

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 zarządzanie 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.**
12. **Podsumowanie kursu. Odpowiedzi na pytania uczestników.**

KURS zakończy się egzaminem, sprawdzającym wiedzę!



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.



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.

Kurs: Ochrona informacji niejawnych w instytucji. Przetwarzanie informacji niejawnych, bezpieczeństwo teleinformatyczne. Niezbędne procedury i praktyka



Kurs będziemy realizowali w formie webinarium on line.



31 maja, 1 i 2 czerwca 2022 r. Kurs w godzinach: 9.00 – 13.30



Cena: 740 PLN netto/os. Udział w kursie zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera: udział w profesjonalnym szkoleniu on-line, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia, możliwość konsultacji z trenerem.

DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej Podkarpacki Ośrodek Samorządu Terytorialnego
ul. Kolejowa 1, 35 – 073 Rzeszów
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 certyfikat w formie: Papierowej
Elektronicznej e mail.....

Proszę o przesłanie faktury na adres mailowy:

Dokonanie zgłoszenia na kurs jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora www.frdl.rzeszow.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przestać poprzez formularz zgłoszenia na www.frdl.rzeszow.pl do 27 maja 2022 r.
UWAGA Liczba miejsc ograniczona. O udziale w kursie decyduje kolejność zgłoszeń. Zgłoszenie na kurs 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 _____