

KURS: OCHRONA INFORMACJI NIEJAWNYCH W INSTYTUCJI



CELE I KORZYŚCI

Uczestnictwo w 3 dniowym kursie zapewni Państwu kompleksową wiedzę i pozwoli nabyć praktyczne, niezbędne umiejętności. W trakcie kursu dowiedzą się Państwo jak właściwie przetwarzać i chronić informacje niejawne; jak zapewnić bezpieczeństwo teleinformatyczne racjonalizując koszty, jak przygotować i nadzorować niezbędne procedury i dokumentację niejawną.

Efekty kursu:

- Podniesienie wiedzy i nabycie praktycznych umiejętności uczestników w zakresie zastosowania wymagań, które są określone w ustawie o ochronie informacji niejawnych i wprowadzenia ich w życie w jednostce, instytucji na przykładzie konkretnych rozwiązań, wzorów, czy wskazówek, pochodzących z wieloletniej praktyki eksperta, wynikającej z jego wykształcenia i doświadczenia zawodowego.
- **Nabycie i udoskonalenie przez uczestników umiejętności opracowania i wdrożenia w jednostce niezbędnej dokumentacji z zakresu OIN, wymaganej ustawą.**
- Wskazanie jak prawidłowo przetwarzać informacje niejawne w jednostce i stosować środki bezpieczeństwa fizycznego w celu ich ochrony, tak, aby skutecznie je zabezpieczyć, racjonalnie gospodarując przy tym środkami finansowymi.
- Zdobycie wiedzy: 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? Jak je archiwizować? Jakie zasady ochrony informacji niejawnych, w tym reguły związane ze stosowaniem przepisów o RODO, stosować w celu prawidłowego funkcjonowania systemu w jednostce/instytucji?
- **Przegląd 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, a także z innymi uczestnikami.

WAŻNE INFORMACJE O SZKOLENIU:

Podczas kursu ekspert w sposób przejrzysty omówi problemy związane z właściwą organizacją pracy kancelarii materiałów niejawnych, ewidencji dokumentów oraz zasad ich przechowywania czy archiwizacji.

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

Udział w 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 praktycznych aspektów.

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



DZIEŃ I. 5 GRUDNIA

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,
 - 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 postępowań sprawdzających – zawartość, przechowywanie i udostępnianie.
9. Obowiązki informacyjne kierownika jednostki organizacyjnej i pełnomocnika ochrony.
10. Karty informacyjne – zasady przesyłania ich do ABW.

Dzień II. 6 GRUDNIA

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 urzędzeń 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. 8 GRUDNIA

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 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.

KURS zakończy się egzaminem, 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 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



Kurs będziemy realizowali w formie webinarium on line.



5, 6 i 8 grudnia 2022 r. Kurs każdego dnia w godzinach: 9.00 – 13.30



Cena: 855 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 Ośrodek Regionalny w Zielonej Górze
al. Niepodległości 16/9, 65 – 048 Zielona Góra
tel. 68 453 22 09, e-mail: szkolenia.zg@frdl.org.pl,
www.zg.frdl.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:

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.zg.frdl.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.zg.frdl.pl do 1 grudnia 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 _____