Ochrona informacji niejawnych

Jakie są obowiązki pełnomocnika ochrony informacji niejawnych w gminie? Jak prowadzić ewidencję materiałów niejawnych krok po kroku? Jak chronić materiały niejawne przed zagrożeniami cybernetycznymi?

Wideoszkolenie PCC Poland skierowane do pełnomocników ochrony informacji niejawnych oraz do innych osób zajmujących się ochroną informacji niejawnych pełniących swoje obowiązki w Urzędach Miast i Gmin.

Jak przetwarzać informacje niejawne w systemie teleinformatycznym krok po kroku?
Uczestnicy dowiedzą się czego dotyczą informacje niejawne, pod jakie klauzule tajności mogą podlegać oraz jak je przetwarzać w sposób fizyczny i elektroniczny. Prowadzący dokładnie omówi procedury weryfikacji potrzebnej do udzielenia osobie dostępu do informacji niejawnych oraz jak te informacje poprawnie zabezpieczać. Ponadto, uczestnicy dowiedzą się jak prowadzić ewidencję dokumentacji niejawnej i co grozi za nieautoryzowane udostępnienie informacji niejawnych do informacji publicznej.

W programie m.in.:

- Jakie są typy klauzuli informacji niejawnych?
- Które postępowania dotyczące informacji niejawnych podlegają rozwiązaniu przez pełnomocnika ochrony informacji niejawnych, a które przez ABW?
- Czy istnieje możliwość tworzenia planu operacyjnego dokumentu zastrzeżonego za pomocą pisma niestałego (na przykład za pomocą ołówka)?
- Jakie wymagania musi spełniać sprzęt komputerowy, aby móc na nim przetwarzać materiały niejawne?
- W jakiej formie powinny być wysyłane i odbierane dokumenty z informacjami niejawnymi drogą elektroniczną?
- Co grozi za udostępnienie informacji niejawnych?
- Na jakich warunkach i na jakiej konkretnie podstawie prawnej istnieje obowiązek przechowywania teczek z informacjami o osobach zajmujących się informacjami niejawnymi przez 20 lat - od daty ich wytworzenia, archiwizowania, czy od czasu, kiedy danej osobie wygasły poświadczenia bezpieczeństwa?

Szczegółowy program szkolenia:

1. Ramy prawne, organizacja pionu ochrony i uprawnienia dostępu

1.1 Regulacje prawne i pojęcia podstawowe

- Czego dotyczą informacje niejawne?
- Jakie są typy klauzuli informacji niejawnych?
- Jakie są warunki wynikające z ustawy dotyczące przetwarzania danych na poziomie zastrzeżonym?
- Jakie są podstawy prawne, aby wydać decyzję o odmowie przy rozpatrywaniu wniosków o udostępnienie informacji publicznej dotyczące informacji niejawnych?
- Na jakich warunkach i na jakiej konkretnie podstawie prawnej istnieje obowiązek przechowywania

teczek z informacjami o osobach zajmujących się informacjami niejawnymi przez 20 lat - od daty ich wytworzenia, archiwizowania, czy od czasu, kiedy danej osobie wygasły poświadczenia bezpieczeństwa?

1.2 Zadania, status i obowiązki pełnomocnika ochrony informacji niejawnych

- Jakie są obowiązki pełnomocnika ochrony informacji niejawnych w gminie?
- Jakie warunki trzeba spełnić, żeby stać się pełnomocnikiem ochrony informacji niejawnych?
- Czy w każdej jednostce organizacyjnej, w której są przetwarzane dokumenty niejawne, powinien być wyznaczony pełnomocnik?
- Jak wygląda proces powoływania pionu do ochrony informacji niejawnych w jednostkach samorządu terytorialnego?
- Jak dokładnie wygląda proces przekazania dokumentacji niejawnej przy zmianie osoby pełniącej stanowisko pełnomocnika ochrony informacji niejawnych?
- Które postępowania dotyczące informacji niejawnych podlegają przeprowadzeniu przez pełnomocnika ochrony informacji niejawnych, a które przez ABW?

1.3 Postępowania sprawdzające i uprawnienia do dostępu

- Jakie warunki powinny spełnić osoby, które chcą uzyskać dostęp do informacji niejawnych i do jakiej klauzuli tajności będą te informacje kwalifikowane?
- Kto udziela dostępu do poszczególnych typów informacji niejawnych?
- Kto powinien otrzymywać upoważnienia dostępu do informacji zastrzeżonej?
- Kto wydaje poświadczenie bezpieczeństwa o dopuszczenie członków jednostek samorządu terytorialnego jak radnych czy członków rady miasta/gminy do informacji niejawnych?
- Ile osób powinno mieć poświadczenia bezpieczeństwa w zależności od wielkości jednostki?
- Jakie są etapy postępowań sprawdzających w celu wydania poświadczenia bezpieczeństwa?
- Jak powinna poprawnie przebiegać procedura prowadzenia postępowania przez pełnomocnika o wydanie poświadczenia bezpieczeństwa?
- Postępowanie dotyczące pozyskiwania poświadczeń bezpieczeństwa przez pracowników - do jakich instytucji trzeba się zgłosić, aby pracownik mógł być odpowiednio zweryfikowany?
- Kwestia wydawania upoważnień dostępu do informacji niejawnych w przypadku wcześniejszej odmowy - czy jeżeli została komuś wydana odmowa takiego dostępu do informacji niejawnych w przeszłości, to czy taka osoba ma prawo uzyskać ten dostęp w przyszłości?

1.4 Szkolenia z zakresu ochrony informacji niejawnych

- Jak wygląda procedura, wedle której pełnomocnik ochrony informacji niejawnych może przeprowadzić szkolenie?
- Czy pełnomocnik może przeprowadzać szkolenia z ochrony informacji niejawnych w zakresie Unii Europejskiej i NATO?

2. Tradycyjny obieg, ewidencja i organizacja kancelarii niejawnej

2.1 Tworzenie, oznaczanie i forma dokumentacji niejawnej

- Jak tworzyć dokumentację niejawną?
- W jaki sposób oznaczyć dokumenty niejawne?
- W jakiej formie można sporządzać dokumenty niejawne oraz jak je przekazywać i odbierać?
- Czy istnieje możliwość tworzenia planu operacyjnego dokumentu zastrzeżonego za pomocą pisma niestałego (na przykład za pomocą ołówka)?

- Czy dokumenty dotyczące stanowiska BSK (Bezpiecznego Stanowiska Komputerowego) mogą być tworzone za pomocą ołówka?

2.2 Rejestracja, księgi ewidencyjne i obsługa kancelaryjna

- Jak prowadzić ewidencję materiałów niejawnych krok po kroku?
- Jak rejestrować pisma zastrzeżone?
- Jak poprawnie prowadzić księgi kancelarii niejawnych z dokumentami zastrzeżonymi?
- Jak poprawnie wpisywać dane do ewidencji dzienników informacji zastrzeżonych?
- Jak poprawnie wypełniać dokumenty i rejestry wymagane do obsługi informacji niejawnych?
- Jakie wzory dokumentów powinny się znajdować w urzędach, w których są przetwarzane informacje niejawne?
- Czy każdy plik zawierający informacje zastrzeżone powinien być zarejestrowany jako jeden plik całościowy, czy jako załączniki do innych dokumentów zarejestrowane pod innymi numerami?

2.3 Organizacja kancelarii, procedury obiegu i przechowywanie

- Jak sporządzić dokumentację dotyczącą organizacji kancelarii niejawnej?
- Jak poprawnie prowadzić kancelarię niejawną?
- Jak powinna przebiegać procedura obiegu dokumentów niejawnych?
- Jakie są zasady przesyłania i odbioru korespondencji oraz dokumentów zawierających informacje niejawne?
- Jak przyjmować korespondencję o różnych stopniach niejawności krok po kroku?
- Jak poprawnie przekazywać informacje w temacie obsługi kancelaryjnej informacji niejawnych krok po kroku?
- Jakie są etapy i przebieg przetwarzania dokumentacji informacji niejawnych krok po kroku?
- Jak poprawnie przechowywać dokumenty niejawne?

3. Bezpieczeństwo teleinformatyczne i systemy elektroniczne

3.1 Przetwarzanie danych oraz wymagania dla sprzętu komputerowego

- Jak przetwarzać informacje niejawne w systemie teleinformatycznym krok po kroku?
- Jak zorganizować środowisko informatyczne, aby móc przetwarzać informacje niejawne w sposób zabezpieczony?
- Jakie wymagania musi spełniać sprzęt komputerowy, aby móc na nim przetwarzać materiały niejawne?
- Na jakim sprzęcie powinny zostać sporządzone dokumenty dotyczące organizacji kancelarii niejawnej?
- W jaki sposób powinny być przechowywane dokumenty elektroniczne dotyczące organizacji kancelarii niejawnej?

3.2 Elektroniczny obieg dokumentów i cyfrowe dzienniki ewidencyjne

- Czy będą możliwe i w jaki sposób będą prowadzone dzienniki ewidencyjne w systemie elektronicznym?
- Prowadzenie książki ewidencji dokumentów niejawnych w formie elektronicznej - jak taka ewidencja powinna być prowadzona oraz w jakim programie ją przeprowadzać?
- W jaki sposób będzie wyglądało potwierdzenie odbioru dokumentów w elektronicznym dzienniku?
- W jakiej formie powinny być wysyłane i odbierane dokumenty z informacjami niejawnymi drogą elektroniczną?

- Czy dokumenty zastrzeżone można wysyłać drogą elektroniczną (przykładowo poprzez e-doręczenia)?

3.3 Akredytacja, certyfikacja i dokumentacja bezpieczeństwa (BSK, SWB i PBE)

- Jak wygląda proces akredytacji sprzętu teleinformatycznego?
- Jak poprawnie prowadzić dokumentację związaną z akredytacją sprzętu komputerowego?
- Jakie wymogi powinno spełniać bezpieczne stanowisko komputerowe do przetwarzania informacji niejawnych o klauzuli zastrzeżone?
- Jak powinna przebiegać certyfikacja stanowiska komputerowego do przetwarzania informacji niejawnych?
- Jak tworzyć dokumentację SWB i PBE?
- Jak utworzyć dokument dotyczący zapewnienia bezpieczeństwa teleinformatycznego?
- Czy powinno się odrębnie rejestrować dysk twardy, na którym się będą znajdować informacje niejawne?

4. Ochrona fizyczna, zarządzanie ryzykiem i odpowiedzialność prawna

4.1 Ochrona fizyczna obiektów i strefy bezpieczeństwa

- Jak chronić budynek zawierający informacje zastrzeżone?
- Jakie są wymagania pomieszczenia, w którym mają być przechowywane informacje tajne?
- Kiedy należy stosować strefy bezpieczeństwa dla miejsc, w których jest praca na dokumentach niejawnych?

4.2 Oszacowanie ryzyka i identyfikacja zagrożeń

- Jakie są możliwe zagrożenia dla informacji niejawnych i zastrzeżonych?
- Jakie są podstawowe kryteria do podziału zagrożeń co do oszacowania ryzyka?
- Jak chronić materiały niejawne przed zagrożeniami cybernetycznymi?
- Jak chronić materiały niejawne przed działaniami dywersyjnymi?

4.3 Plany ochrony i procedury zabezpieczeń

- Jak funkcjonuje system obiegu oraz zabezpieczeń informacji niejawnej?
- Jak poprawnie zabezpieczyć informacje niejawne krok po kroku?
- Jak powinien wyglądać plan ochrony informacji niejawnych krok po kroku?
- Jak stworzyć plan ochrony informacji zastrzeżonych?
- Jak przetwarzać informacje niejawne?

4.4 Naruszenia procedur i odpowiedzialność karna oraz dyscyplinarna

- Co powinno zawierać postępowanie wyjaśniające naruszenia informacji niejawnych i jak je prawidłowo przeprowadzić?
- Jak będzie wyglądać odpowiedzialność karna i dyscyplinarna za naruszenie dostępu do informacji niejawnych?
- Co grozi za udostępnienie informacji niejawnych?

5. Archiwizacja, zarządzanie klauzulami oraz procedury kryzysowe i obronne

5.1 Zmiana, znoszenie klauzul i zarządzanie cyklem życia dokumentów

- Jak przeprowadzić zmiany klauzul tajności i jak te klauzule usuwać?

- Jak przeprowadzić odtajnianie dokumentów zastrzeżonych?
- Jakie są podstawy, aby odtajnić dokument, który powstał przed utworzeniem jednostek samorządu terytorialnego?
- Jak zlikwidować lub wycofywać dokumenty niejawne wydanych przez nieistniejące już instytucje?
- Czy dokumenty oznaczone klauzulą niejawności w przypadku braku zapotrzebowania na jego używanie mogą być odesłane do osoby, która wystawiła tę klauzulę czy trzeba je nadal przechowywać?

5.2 Klasyfikacja i procedury archiwizacji

- Jak przeprowadzić archiwizację dokumentów niejawnych krok po kroku?
- Jak kwalifikować, które stare dokumenty niejawne podlegają archiwizacji?
- Archiwizacja materiałów niejawnych na dyskach twardych lub dyskach USB - jak ją przeprowadzić i czy dysk z takimi danymi można zniszczyć komisyjnie?

5.3 Obronność, sytuacje kryzysowe i ewakuacja

- W jaki sposób będą tworzone systemy przekazywania informacji niejawnych w czasie kryzysu i w czasie wojny i jak ma to wyglądać w samorządzie gminnym?
- Przypadek: jak w czasie podwyższonej gotowości obronnej trzeba będzie przeprowadzić ewakuację informacji niejawnych, gdy pełnomocnik jest zatrudniony na pół etatu w dwóch gminach?

Prowadzący:

Prelegent pełni funkcję pełnomocnika ds. ochrony informacji niejawnych od 2010 roku.

Zajmuje się tematyką ochrony informacji niejawnych od roku 2000, kiedy pełniąc funkcję oficera Wojska Polskiego został wyznaczony na nowo powstałe stanowisko pełnomocnika ds. ochrony informacji niejawnych. Budował pion ochrony informacji niejawnych w jednostce wojskowej wdrażając zapisy Ustawy o ochronie informacji niejawnych.

Studiował i ukończył Wyższą Szkołę Oficerską Wojsk Rakietowych i Artylerii w latach 1979-1983 uzyskując tytuł podporucznika, Wyższą Szkołę Pedagogiczną w latach 1995-1998 uzyskując tytuł magistra wychowania obronnego oraz studia podyplomowe w zakresie bezpieczeństwa i higieny pracy w latach 2005-2006.