

PROCEDURY REAGOWANIA NA INCYDENTY NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH I INFORMACJI W SYSTEMACH TELEINFORMATYCZNYCH JAKO ELEMENT KONTROLI ZARZĄDCZEJ

WAŻNE INFORMACJE O SZKOLENIU:

Przedmiotem proponowanego szkolenia jest przeanalizowanie krok po kroku problematyki procedur bezpiecznego przechowywania informacji w systemach teleinformatycznych jako elementu zarządzania w jednostce. Omówimy przykładowe procedury i rozwiązania dotyczące bezpieczeństwa informacji w kontekście reagowania na incydenty zgodnie z przepisami ustawy o KSC i ustawy o ochronie danych osobowych.

Podczas zajęć odpowiemy na pytania dotyczące m.in.:

- Jakie obowiązki związane z bezpieczeństwem informacyjnym spoczywają na kierowniku jednostki organizacyjnej w ramach kontroli zarządczej?
- W jaki sposób ustalić klasyfikację informacji w systemach teleinformatycznych?
- W jaki sposób postępować w przypadku zdarzenia a w jaki sposób reagować na incydent?
- Jaka jest rola osoby wyznaczonej w jednostce do kontaktu w ramach Krajowego Systemu Cyberbezpieczeństwa?
- Czy należy dokonać analizy ryzyka zabezpieczeń informacji w systemach teleinformatycznych?
- Jaka jest rola obsługi informatycznej związanej z zabezpieczeniami informacji a jaka rola kierownictwa jednostki organizacyjnej?

Zajęcia prowadzone będą częściowo w formie prezentacji multimedialnej, warsztatów a także dyskusji angażującej uczestników przy rozwiązywaniu przypadków przygotowanych w oparciu o faktycznie zaistniałe sytuacje.

CELE I KORZYŚCI:

- Rzeczywiste zorientowanie jednostki na efektywne zarządzanie informacjami. Zdobyć, uzupełnienie i uporządkowanie wiedzy w przedmiotowym zakresie.
- Wskazanie metod tworzenia w jednostce struktury reagowania na incydenty i zdarzenia związane z bezpieczeństwem informacji.
- Poznanie zasad wcześniejszej identyfikacji ryzyk i możliwość szybkiego na nie reagowania, co powinno przełożyć się na mniejszą ilość nieprawidłowości pojawiających się w funkcjonowaniu jednostki.
- Wskazanie elementów skutecznego funkcjonowania systemu kontroli zarządczej oraz realizacja ustawowych obowiązków reagowania na incydenty bezpieczeństwa w systemach teleinformatycznych oraz incydenty bezpieczeństwa danych osobowych.
- Omówienie procedury zgłaszania incydentów bezpieczeństwa do CSIRT NASK i UODO.
- Zaprezentowanie całościowego i skutecznego podejścia do zarządzania bezpieczeństwem informacji w jednostce.
- Zdobyć umiejętności identyfikacji podatności i analizy ryzyka informacji i danych osobowych w systemach teleinformatycznych.
- Realizacja ustawowego obowiązku wynikającego z Ustawy o Krajowym Systemie Cyberbezpieczeństwa i Ustawy o ochronie danych osobowych.

- Zdobyć wiedzę na temat skutecznych i efektywnych procedur zmniejszających ryzyko utraty informacji i danych osobowych.
- Poznanie i możliwość wdrażania procedury działania w razie zaistnienia incydentu oraz planu naprawczego.
- Uzyskanie odpowiedzi na najczęściej pojawiające się pytania i wątpliwości z zakresu przedmiotu zajęć.

PROGRAM:

1. Definicje prawne, definicja zdarzenia i incydentu bezpieczeństwa:
 - Rodzaje systemów teleinformatycznych.
 - Klasyfikacja przetwarzanych informacji w systemach teleinformatycznych.
2. Bezpieczeństwo informacji a system kontroli zarządczej w jednostki.
3. Incydent a zdarzenie:
 - Podstawowe różnice znaczeniowe.
 - Adekwatne działanie i reakcja.
4. Incydenty w systemach jawnych:
 - Incydenty związane z naruszeniem bezpieczeństwa danych osobowych.
 - Incydenty związane z naruszeniem bezpieczeństwa informacji.
5. Incydenty w systemach niejawnych:
 - Rodzaje incydentów.
 - Wdrażane procedury.
6. Tworzenie zespołów reagowania na incydenty bezpieczeństwa:
 - Skład, struktura i zadania zespołu.
 - Zarządzanie zespołem reagowania.
7. Procedury zmniejszające ryzyko utraty informacji i danych osobowych:
 - Prawdopodobieństwo wystąpienia sytuacji niepożądaney.
 - Zagrożenia bezpieczeństwa informacyjnego.
 - Dobór środków przeciwdziałania.
 - Ryzyko akceptowalne.
8. Plany reakcji na incydenty:
 - Procedury działania w razie wystąpienia incydentu.
 - Aktualizacja i monitorowanie procedur.
 - Scenariusze reagowania na incydenty.
 - Wdrażanie planu naprawczego – po wystąpieniu incydentu.
9. Podsumowanie. Dyskusja.

ADRESACI:

Szkolenie skierowane do Kadry zarządzającej wyższego szczebla, wójtów, burmistrzów, sekretarzy, dyrektorów, pracowników wykonujących obowiązki w ramach kontroli zarządczej. Szkolenie jest przeznaczone dla osób zarządzających jednostkami organizacyjnymi o różnym poziomie zaawansowania wiedzy i doświadczenia w zakresie bezpieczeństwa informacyjnego.

PROWADZĄCY:

Prawnik, doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie. Posiada wieloletnie doświadczenie zawodowe na stanowisku Pełnomocnika Ochrony Informacji Niejawnych w samorządzie terytorialnym, Kierownika kancelarii materiałów niejawnych oraz inspektora bezpieczeństwa teleinformatycznego. Biegły sądowy w zakresie ochrony informacji niejawnych i tajemnic prawnie chronionych przy Sądzie Okręgowym.

Procedury reagowania na incydenty naruszenia bezpieczeństwa danych osobowych i informacji w systemach teleinformatycznych jako element kontroli zarządczej



Szkolenie będziemy realizowali w formie webinarium on line.



7 lipca 2023 r.

Szkolenie w godzinach 10:00-14:30



on-line

Wirtualne szkolenie prowadzone i realizowane na żywo za pomocą platformy zoom, która umożliwia obustronną komunikację między prowadzącym szkolenie a uczestnikami.

Cena udziału w szkoleniu wynosi 395 PLN netto/os.

Cena obejmuje: Udział w profesjonalnym szkoleniu on-line z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.



stacjonarnie

MIEJSCE: As-Bud Centrum Konferencyjno-Szkoleniowe; al. Jerozolimskie 81; 02-001 Warszawa.

Cena 569 PLN netto/os.

Cena obejmuje: Udział w profesjonalnym szkoleniu stacjonarnym z możliwością zadawania pytań, materiały szkoleniowe w wersji papierowej, certyfikat ukończenia szkolenia, przerwa kawowa i lunch.

Organizator nie zapewnia miejsc parkingowych.

Zgłaszam udział w szkoleniu w formule:

Stacjonarnej On-line

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

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.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 lipca 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 _____