

Czy nowatorska ochrona informacji (zgodna z normą PN-ISO/IEC-27001:2007) ma wpływ na wzrost zysku firmy lub upadek firmy?

Cele szkolenia:

- podniesienie świadomości Managementu Firmy wobec szeregu współczesnych, nieznanych zagrożeń utraty czy modyfikacji cennych aktywów informacyjnych oraz zapoznanie się z podstawowymi rodzajami zagrożeń i metodami zabezpieczeń przed tymi zagrożeniami.
- zaprezentowanie Managementowi związku pomiędzy zasadnością wdrożenia zgodnej z normami profesjonalnej ochrony informacji a kluczową, niedocenianą rolą „czynnika ludzkiego” oraz zyskiem i wzrostem konkurencyjności firmy.

Korzyści z uczestnictwa w szkoleniu:

- Przypomnienie ogólnych wytycznych prawnych ochrony informacji oraz sankcji wynikających z ich niestosowania, a także korzyści wynikających z ich wdrożenia
- Zapoznanie się z wytycznymi normy PN-ISO/IEC-27001:2007 oraz norm związanych
- Zapoznanie Managementu firmy z celami i korzyściami wynikającymi z wdrożenia Polityki Bezpieczeństwa oraz procedur i zapisów o globalnej ochronie wszelkich cennych aktywów informacyjnych firmy
- Umiejętność pokierowania w swojej firmie całym procesem zmian, zmierzających do uzyskania wartości dodanej – świadomego i twórczego przywództwa w kompleksowym wdrażaniu w swojej firmie profesjonalnej ochrony informacji, zgodnej z normą PN-ISO/IEC-27001:2007
- Uzyskanie imiennych certyfikatów przez uczestników szkolenia

Business People Alignment



Uczestnicy szkolenia:

Szkolenie dedykowane jest wyłącznie dla Kadry Zarządzającej firm zainteresowanych:

- zwiększeniem bezpieczeństwa swoich aktywów informacyjnych
- podkreśleniem, że ludzie dbający o wszelkie informacje firmy to największe jej dobro
- innowacyjnymi sposobami zwiększenia bezpieczeństwa swoich cennych informacji oraz bezpieczeństwa firmy
- autentycznym, świadomym przywództwem w swojej firmie we wdrożeniu normy PN-ISO/IEC-27001:2007
- bezpiecznym zyskiem firmy w kontekście ochrony informacji,
- zwiększeniem konkurencyjności swojej firmy,
- inwestycją w świadomą ochronę informacji wśród swoich pracowników.

Metoda szkolenia:

Szkolenie prowadzone jest metodą wykładowo - prezentacyjną, z aktywnym uczestnictwem słuchaczy w dyskusjach na wybrane tematy

Zakres szkolenia:

Moduł 1: Bezpieczeństwo Informacji

- Nowa, rozszerzona definicja informacji we współczesnym świecie
- Podstawy prawne ochrony aktywów przedsiębiorstwa
- Pojęcie wielowątkowego, kompleksowego Bezpieczeństwa Informacji
- Klasyfikacja zagrożeń, incydenty naruszenia bezpieczeństwa
- Incydenty bezpieczeństwa - skutki bezpośrednie i pośrednie
- Metody i reguły perfidnego oddziaływania socjotechników na naszych pracowników oraz praktyczne sposoby obrony i ochrony przed nimi

Moduł 2: Norma PN-ISO/IEC 27001:2007 w moim przedsiębiorstwie

- Najważniejsze elementy normy, aspekty zarządzania procesowego
- Zalecana kolejność i metodyka wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (ISMS) zgodnego z w/w normą
- Deklaracja Stosowania – wentyl bezpieczeństwa dla każdego wdrożenia
- Praktyczna rola Kierownictwa firmy w inicjowaniu i nadzorowaniu wdrożenia normy oraz cyklicznym jej przeglądzie

Business People Alignment



- Certyfikacja zewnętrzna na zgodność z normą – zalety i korzyści
- Inne normy związane

Moduł 3: Audyt oraz Polityka Bezpieczeństwa wg normy PN-ISO/IEC 27001:2007

- Audyt Bezpieczeństwa Firmy wg normy PN-ISO/IEC 27001:2007
- Audytorzy wewnętrzni – predyspozycje, odpowiedzialność, raporty, zapisy
- Przebieg audytu – najlepsze praktyki, zalecenia eksperckie
- Budowa Kompleksowej Polityki Bezpieczeństwa Firmy
- Zespół Wdrożeniowy – przypadek, czy świadomy wybór?
- Odniesienia do istniejących Polityk a nowe regulacje

Moduł 4: Kluczowa rola tzw. “czynnika ludzkiego”

- Iloczynowe znaczenie czynnika ludzkiego i jego wpływ na sukces wdrożenia
- Zagrożenia dla czynnika ludzkiego
- Autentyczny przykład Kierownictwa, zarządzanie motywacją godnościową, etos pracowniczy
- Rola i miejsce „czynnika ludzkiego” w Polityce Bezpieczeństwa
- Podsumowanie treści szkolenia

Czas trwania – 1 dzień, (ok. 5 godzin)

Business People Alignment

