04

EDUKACJA I BUDOWANIE ŚWIADOMOŚCI - SZKOLENIA

Szkolenia dla użytkowników z zakresu ochrony danych osobowych.

Szkolenia z zakresu zarządzania ryzykiem IT.

Szkolenia dla użytkowników z zakresu bezpieczeństwa informacji.

Szkolenia dla Administratorów.

Szkolenia dla Kadry Zarządzającej.

Egzamin końcowy i certyfikaty dla uczestników szkoleń.

www.coig.pl

§

***OBOWIĄZEK** zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok wynika bezpośrednio z ROZPORZĄDZENIA RADY MINISTRÓW z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (§20, ust.2, pkt 14).*

§

***OBOWIĄZKIEM** Administratora Bezpieczeństwa Informacji jest okresowe sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania (Rozdział 5, Art. 36a, ust. 2, pkt 1 Ustawy o Ochronie Danych Osobowych).*

COIG S.A.
ul. Mikołowska 100
40-065 Katowice

www.coig.pl

COIG

MONITORING STANU ZAGROŻEŃ DLA BEZPIECZEŃSTWA IT

SYSTEM JEST TAK BEZPIECZNY

JAK ŚWIADOMI SĄ JEGO UŻYTKOWNICY

01

OCHRONA DANYCH OSOBOWYCH - AUDYT

- Analiza procesów związanych z przetwarzaniem danych osobowych.
- Identyfikacja zbiorów danych osobowych.
- Identyfikacja systemów informatycznych przetwarzających dane osobowe.
- Weryfikacja zabezpieczeń logicznych i fizycznych do wydzielonych zasobów informatycznych przeznaczonych do przetwarzania danych osobowych.
- Weryfikacja dokumentacji związanej z ochroną danych osobowych.
- Ocena zgodności z Ustawą o Ochronie Danych Osobowych.
- Wykonanie raportu poaudytowego.

02

AKTYWNY MONITORING INFRASTRUKTURY IT – USŁUGA W TRYBIE CIĄGŁYM

- Rejestrowanie i obsługa incydentów bezpieczeństwa.
- Okresowe badanie podatności systemów i elementów infrastruktury.
- Analiza powłamaniowa.
- Tworzenie i utrzymywanie polityk ochrony systemów i sieci.
- Analiza i zarządzanie ryzykiem w systemach IT.

03

BEZPIECZEŃSTWO FUNKCJONOWANIA ORGANIZACJI - AUDYT

- Ewidencja elementów środowiska IT.
- Weryfikacja procedur i procesów funkcjonujących w ramach Działu IT.
- Weryfikacja dokumentacji systemowej oraz infrastruktury teleinformatycznej.
- Weryfikacja polityki bezpieczeństwa Organizacji.
- Identyfikacja i wykrycie nieuprawnionych dróg dostępu do systemów działających w Organizacji.
- Analiza wykorzystania urządzeń mobilnych i nośników danych.
- Identyfikacja i weryfikacja działania narzędzi dla ochrony przed złośliwym oprogramowaniem.
- Analiza zagrożeń dla ciągłości działania Organizacji.
- Kontrola zabezpieczeń przed utratą danych.
- Weryfikacja sposobu zarządzania incydentami bezpieczeństwa.
- Propozycje działań naprawczych i prewencyjnych.
- Wykonanie raportu poaudytowego.