ATFIDE
GRUPA PRAWNA

Oferta na;

Przeprowadzenie audytu Systemu Zarządzania Bezpieczeństwem Informacji

w jednostkach sektora publicznego

na zgodność z wymaganiami ust. 1 i 2 § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r. poz. 526)

Szanowni Państwo,

Firma ATFIDE Sp. z o.o., dzięki odpowiednio dobranemu, profesjonalnemu zespołowi specjalistów ds. bezpieczeństwa i ochrony informacji, opracowała dla Państwa ofertę, w zakresie przeprowadzenia **niezależnego audytu bezpieczeństwa Systemu Zarządzania Bezpieczeństwem Informacji** w Państwa Jednostce.

Przypominamy, **że spoczywa na Państwu obowiązek** dostosowania się do przepisów rozporządzenia KRI, oraz do **zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok w swojej Jednostce**.

Warto w tym miejscu podkreślić, iż Najwyższa Izba Kontroli przeprowadza już kontrole badające dostosowanie instytucji i jednostek, w ramach realizacji nowych wymagań określonych w rozporządzeniu KRI.

Podstawy prawne realizacji usługi:

- *Rozporządzenie rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych(Dz. U. z 2012r. poz. 526)*

Zakres usługi:

1. Ocena procedur i regulacji wewnętrznych uwzględniających wymagania rozporządzenia „Krajowe Ramy Interoperacyjności”.(Dz. U. z 2012r. poz. 526).

2. Analiza spełnienia minimalnych wymagań dla systemów teleinformatycznych:

- utrzymania / zarządzania systemami IT,
- wymiany danych z innymi systemami i kodowania znaków,
- dostosowania systemów do standardów WCAG2.0 (kwestia większej dostępności dla osób niepełnosprawnych),
- wymagań dotyczące bezpieczeństwa,

3. Analiza spełnienia minimalnych wymagań bezpieczeństwa:

- zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia tj. przygotowanie odpowiednich procedur, zabezpieczenie systemów, wprowadzenie odpowiednich mechanizmów monitoringu bezpieczeństwa,
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
- podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
  - zagrożenia bezpieczeństwa informacji,
  - skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
  - stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
  - monitorowanie dostępu do informacji
  - czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji
  - zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
- zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
- zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
  - dbałości o aktualizację oprogramowania,
  - minimalizowaniu ryzyka utraty informacji w wyniku awarii,
  - ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
  - stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
  - zapewnieniu bezpieczeństwa plików systemowych,
  - redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
  - niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
  - kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

5. Weryfikacja przyjętych procedur i zasad bezpieczeństwa informacji, zapobiegająca osobom nieuprawnionym ich ujawnienie, modyfikacje, usunięcie lub zniszczenie oraz umożliwiających szybkie podjęcie działań korygujących

Wyniki realizacji usługi audytu:

Opracowanie raportu dokumentującego jego przebieg wraz z informacjami o spostrzeżeniach i uchybieniach w odniesieniu do spełnienia wymagań ust. 1 i 2 § 20 Rozporządzenia, stanowiących podstawę do podjęcia przez instytucję działań przywracających zgodności z wymaganiami. Raport zawiera w szczególności uwagi, wnioski, zalecenia i wytyczne w celu rozpoznania i ograniczenia zidentyfikowanych ryzyk, zagrożeń i podatności obszarów oraz wskazanie adekwatnych działań mających na celu jak najszybsze ich wyeliminowanie.

Koszt realizacji usługi: *do uzgodnienia*