Załącznik do zarządzenia nr 6/2011 – Polityka bezpieczeństwa danych osobowych

ZESPÓŁ SZKÓŁ NR 3

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Administrator Danych Osobowych
2011-01-01

I. CZĘŚĆ ZEWNĘTRZNA

Niniejsza część Polityki bezpieczeństwa zawiera ogólnodostępne informacje dotyczące zasad przetwarzania danych osobowych w Zespole Szkół nr 3 i jest dostępna dla każdej zainteresowanej osoby.

1. Definicja bezpieczeństwa informacji

Polityka bezpieczeństwa informacji jest to zestaw praw, reguł i zasad ich tworzenia, sposobów zarządzania, dystrybucji, użytkowania i przechowywania danych osobowych.

Dyrektor wprowadza politykę bezpieczeństwa informacji w celu uświadomienia całej organizacji potrzeby ochrony danych niezależnie od przyjmowanej przez nie formy (dokumenty na dysku, wydrukowane).

Bezpieczeństwo systemów informatycznych odnosi się do wszystkich procesów związanych z informacją to jest: wytwarzania, przetwarzania, przechowywania, archiwizowania, przesyłania, zbierania, prezentowania oraz niszczenia.

2. Deklaracja kierownictwa

Dyrektor angażuje się w rozwój i wdrożenie systemu bezpieczeństwa danych osobowych posiadanych przez Zespół Szkół nr 3 i deklaruje pracę nad stałym doskonaleniem niniejszej polityki.

W Zespole Szkół nr 3 przeprowadzono cykl szkoleń, które obejmowały zagadnienia dotyczące zachowywania przetwarzanych przez Zespół Szkół nr 3 zbiorów danych osobowych w bezpieczeństwie.

Ponadto ustanowiono niniejszą politykę, której znajomość stanowi obowiązek każdego pracownika w Zespole Szkół nr 3.

3. Podstawa prawna

Dokument został stworzony na podstawie ustawy o ochronie danych osobowych z dnia 29 kwietnia 1997 roku z późniejszymi zmianami (Dz. U. 2002 nr 101 poz.926 tekst jednolity) zwanej dalej ustawą i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. zwanego dalej rozporządzeniem [Dz. U.2004 nr 100 poz. 1024].

4. Definicje pojęć

- **Dane osobowe** – każda informacja dotycząca osoby fizycznej pozwalająca na określenie tożsamości tej osoby.

- **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i ich usuwanie.
- **Administrator bezpieczeństwa informacji** – osoba nadzorująca przestrzeganie zasad ochrony przetwarzania danych osobowych.
- **Administrator systemu informatycznego** – osoba odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach;
- **Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem** – osoba posiadająca upoważnienie wydane przez administratora danych dopuszczona, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.
- **Osoba trzecia** – każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu administratora danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez administratora danych podejmująca czynności w zakresie przekraczającym ramy jej upoważnienia.
- **System informatyczny, zwany dalej systemem** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Zabezpieczenie systemu informatycznego** – wdrożenie przez administratora bezpieczeństwa informacji oraz administratora systemu informatycznego stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
- **Zapewnienie bezpieczeństwa systemów informatycznych** oznacza, utrzymanie takich atrybutów informacji jak:
- **Poufność**, która oznacza ograniczony i ściśle zdefiniowany krąg osób mających dostęp do informacji.
- **Integralność**, to jest zapewnienie niezmienności postaci informacji (postać oryginalna), za wyjątkiem momentów, kiedy informacja ta jest w sposób legalny modyfikowana.
- **Autentyczność (informacji, nadawcy, adresata)** – oznacza to zgodność tożsamości informacji (nadawcy, adresata) z deklaracją do niej przypisaną.
- **Dostępność** (informacji) dla wszystkich uprawnionych do tego osób.
- **Rozliczalność** – oznaczająca precyzyjne i jednoznaczne powiązanie każdego dostępu do informacji z właściwą uprawnioną osobą, która tego dokonała
- Niezawodność pracy całości systemu a w szczególności aplikacji i urządzeń zawierających, przetwarzających, przesyłających informacje podlegające ochronie.

System zabezpieczeń systemów informatycznych obejmuje:

- Bezpieczeństwo fizyczne (strefy bezpieczeństwa, zamykane pomieszczenia, szafy pancerne itp.).
- Bezpieczeństwo techniczne.
- Bezpieczeństwo organizacyjno-proceduralne.

II. **W celu zapewnienia ochrony informacji na wymaganym poziomie wykorzystywane są zawsze metody i środki ze wszystkich trzech wymienionych obszarów. Oznacza to kompleksowy charakter zabezpieczeń. Wszystkie trzy wymienione obszary są jednakowo ważnymi elementami realizacji polityki bezpieczeństwa informacji.**