

**REGULAMIN OCHRONY DANYCH OSOBOWYCH**

**Gimnazjum nr 1 im. prof. Jana Szczepańskiego w Ustroniu**

***Ustroń, 2010***

# I. POLITYKA BEZPIECZEŃSTWA

## Pojęcia podstawowe

1. Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych Dz. U. z 2004 r. Nr 100, poz. 1024. Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

1. Regulamin niniejszy określa tryb i zasady ochrony danych osobowych przetwarzanych w Gimnazjum nr 1 im. prof. Jana Szczepańskiego w Ustroniu, zwanym dalej Jednostką.

3. Ilekroć w regulaminie jest mowa o :

1. **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
2. **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tj. uczniów, nauczycieli, innych pracowników i rodziców uczniów;
3. **przetwarzaniu danych -** rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
4. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
5. **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
6. **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7. **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8. **administratorze danych osobowych** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Dyrektora Jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;
9. **użytkowniku systemu informatycznego** - rozumie się przez to upoważnionego przez Dyrektora Jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;

## **Cele**

Celem opracowania polityki bezpieczeństwa jest ochrona przed niepowołanym dostępem do:

1. systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;
2. informacji zgromadzonych, przetwarzanych w formie tradycyjnej.

Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w instytucjach samorządowych dotyczącymi bezpieczeństwa i poufności przetwarzanych danych. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi. Opracowane procedury określają obowiązki użytkownika zbiorów tradycyjnych oraz zasady korzystania z systemów informatycznych. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.

# II. ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

## **Informacje ogólne**

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada administrator danych osobowych, jeżeli został powołany przez Dyrektora. Nauczyciele i inni pracownicy szkoły obowiązani są zastosować środki e zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą utratą uszkodzeniem lub zniszczeniem.

## **OSOBY ODPOWIEDZIALNE ZA ZABEZPIECZENIE DANYCH OSOBOWYCH**

1. Dyrektor Gimnazjum
2. Wicedyrektor Gimnazjum
3. Wychowawcy klas i inni nauczyciele uczący w szkole;
4. Pracownicy sekretariatu.

## **Rodzaje dokumentów zawierających chronione dane osobowe**

**I. Dokumenty zawierające dane osobowe przechowywane w formie tradycyjnej.**

 1. Arkusze ocen uczniów oraz oprawione księgi arkuszy ocen absolwentów i uczniów,

 którzy opuścili szkołę przed jej ukończeniem..

 2. Dzienniki lekcyjne i dzienniki innych zajęć.

 3. Teczki osobowe nauczycieli i innych pracowników szkoły.

 4. Karty zdrowia uczniów.

 5. Księga ewidencji dzieci zamieszkałych w obwodzie szkoły.

 6. Księga uczniów zapisanych do szkoły.

 **II. Zbiory danych osobowych przechowywane w formie elektronicznej**.

 1. Baza uczniów zapisanych do szkoły.

 2. Baza nauczycieli i innych pracowników szkoły.

 3. Dane o nauczycielach i uczniach zawarte w bazie Systemu Informacji Oświatowej.

 4. Oceny pracy oraz oceny dorobku zawodowego nauczycieli i innych pracowników.

## **osoby posiadające dostęp do danych osobowych**

1. Dyrektor i wicedyrektor, a także nauczyciel zastępujący dyrektora w razie jego

 nieobecności.

2. Sekretarka lub referent ds. szkoły.

3. Specjalista ds. BHP

4. Wychowawcy klas i inni nauczyciele szkoły.

5. Kierownik i referent ds. kadr Jednostki Obsługi Placówek Oświatowych przy UM.

6. Rodzice ( opiekunowie prawni ) uczniów – tylko do danych osobowych swoich dzieci.

## **Procedury dostępu do systemu**

1. **Procedury dostępu do systemów tradycyjnych**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Lp.*** | ***Czynność*** | ***Kto*** | ***Uwagi – sposób zabezpieczenia*** |
| **1** | Dostęp do danych osobowych nauczycieli i innych pracowników szkoły, to jest do teczek osobowych. | - Dyrektor, wicedyrektor, osoba zastępująca dyrektora w razie jego nieobecności.- Sekretarka, referent ds. szkoły, specjalista ds. BHP.- Kierownik i referent ds. kadr JOPO. | 1. Szafa w sekretariacie i gabinecie dyrektora zabezpieczona zamkiem, 2. Jak wyżej3. Szafy w UM zabezpieczone przez Kierownika JOPO |
| **2** | Dostęp do danych osobowych uczniów, to jest do wszystkich dokumentów przebiegu nauczania. | - Dyrektor, wicedyrektor, osoba zastępująca dyrektora w razie jego nieobecności.- Sekretarka, referent ds. szkoły, specjalista ds. BHP.- Wychowawcy klas i inni nauczyciele uczące danego ucznia.- Rodzic do danych swojej dziecka, to jest ocen . | 1. Pokój nauczycielki – zamek szyfrowy w drzwiach.2. Szafa w sekretariacie i gabinecie dyrektora zabezpieczona zamkiem |

2. **Procedury dostępu do komputerów, na których zainstalowane są bazy danych**

 **osobowych**.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Komputer – miejsce zainstalowania** | **Kto ma dostęp** | **Uwagi – sposób korzystania, zabezpieczenie.** |
| 1. | Sekretariat – komputer sekretarki | 1. Dyrektor szkoły | Bezpośrednio lub w sieci, Zabezpieczenie : hasło dostępu. |
| 2. Sekretarka | Bezpośrednio-Zabezpieczenie : hasło dostępu. |
| 2. | Gabinet dyrektora | Dyrektor, wicedyrektor, osoba zastępująca dyrektora w razie jego nieobecności | BezpośrednioZabezpieczenie hasło dostępu, nie udostępniony w sieci. |
| 3. | Gabinet wicedyrektora | Dyrektor, wicedyrektor, osoba zastępująca dyrektora w razie jego nieobecności | BezpośrednioZabezpieczenie hasło dostępu, nie udostępniony w sieci. |
| 4. | Sekretariat – komputer specjalisty ds. BHP | Specjalista ds. BHP | BezpośrednioZabezpieczenie hasło dostępu, nie udostępniony w sieci. |
| 5. | Pokój nauczycielski | Wszyscy nauczyciele szkoły | Bezpośrednio, Zabezpieczenie – drzwi zamek szyfrowy, komputer hasło dostępu. |
| 6. | Gabinet pedagoga | Pedagog szkolny | Bezpośrednio, Zabezpieczenie – hasło dostępu. |

Komputery w innych pomieszczeniach ( biblioteka, pracownia komputerowa )

# III. Udostępnianie posiadanych w zbiorze danych osobowych

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest dyrektor, wicedyrektor oraz osoba zastępująca dyrektora w razie jego nieobecności.
2. W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa
3. W przypadku nieuprawnionego ujawnienia danych osobowych zawartych w zasobach szkoły dyrektor podejmuje postępowanie wyjaśniające i stosuje sankcje przewidziane w przepisach prawa.