POLITYKA BEZPIECZEŃSTWA INFORMACJI

oraz

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W I SPOŁECZNYM LICEUM

OGÓLNOKSZTAŁCĄCYM

IM. MAHARADŻY JAM SAHEBA DIGVIJAY SINHJI

W WARSZAWIE

SPIS TREŚCI

Podstawa prawna

1. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101 poz. 926 z późniejszymi zmianami);
2. Rozporządzenie MSW i A 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).

Podstawowe pojęcia stosowane w niniejszym dokumencie

1. Szkoła – I Społeczne Liceum Ogólnokształcące im. Maharadży Jam Saheba Digvijay Sinhji w Warszawie, ul. Zawiszy 13;
2. Polityka bezpieczeństwa – dokument *Polityka bezpieczeństwa informacji* obowiązujący w I Społecznym Liceum Ogólnokształcącym w Warszawie;
3. Instrukcja – *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w I Społecznym Liceum Ogólnokształcącym w Warszawie;*
4. Przetwarzanie danych – zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych;
5. Administrator Danych Osobowych (ADO) – dyrektor I Społecznego Liceum Ogólnokształcącego w Warszawie
6. Administrator Bezpieczeństwa Informacji (ABI) **–** pracownik szkoły powołany zarządzeniem dyrektora I Społecznego Liceum Ogólnokształcącego w Warszawie do przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych oraz nadzoru nad przestrzeganiem zasad ochrony danych osobowych;
7. Użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie;
8. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

I. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I.1. Wykaz budynków, w których przetwarzane są dane osobowe

Lp.	Budynek	Pomieszczenia
	ul. Zawiszy 13 01-167 Warszawa	gabinet dyrektora gabinet wicedyrektorów (sala nr 5) pokój nauczycielski sekretariat/serwerownia gabinet lekarski biblioteka sale lekcyjne

I.2. Zbiory danych osobowych przetwarzanych w systemach informatycznych i opis struktury przetwarzanych danych

ZBIÓR DANYCH OSOBOWYCH	**PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH OSOBOWYCH**	**STRUKTURA DANYCH OSOBOWYCH**
Pracownicy	IDU	Imię i nazwisko, e-mail, numer telefonu
	Bibliotekarz	Imię i nazwisko
Uczniowie	IDU	Imię i nazwisko, PESEL, data i miejsce urodzenia, adres zamieszkania i zameldowania, numer w *Księdze uczniów*, numer legitymacji, imiona i nazwiska rodziców/opiekunów, adres zamieszkania rodziców/opiekunów e-mail rodziców/opiekunów, numer telefonu rodziców/opiekunów numer konta bankowego rodziców/opiekunów
	Bibliotekarz	Imię i nazwisko

I.3. Zbiory danych przetwarzanych tradycyjnie

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUŻĄCA DO PRZETWARZANIA ZBIORU DANYCH OSOBOWYCH	STRUKTURA DANYCH OSOBOWYCH
Pracownicy	Upoważnienia	Imię i nazwisko, numer dowodu osobistego
	Oświadczenia i wnioski do funduszu socjalnego	Imię i nazwisko, PESEL, data i miejsce urodzenia, adres zamieszkania, adres zameldowania, numer telefonu, e-mail, oświadczenie o dochodach
Uczniowie	Dokumentacja indywidualna uczniów	Imiona i nazwisko, PESEL, data i miejsce urodzenia, adres zamieszkania, adres zameldowania, numer telefonu, e-mail, numer legitymacji szkolnej, wyniki na świadectwie ukończenia gimnazjum, wyniki egzaminu gimnazjalnego, informacje o dysfunkcjach, imiona i nazwiska rodziców/opiekunów, telefon rodziców/opiekunów, e-mail rodziców/opiekunów, zawód rodziców/opiekunów, miejsce pracy rodziców/opiekunów
	Dokumentacja indywidualna absolwentów	Imiona i nazwisko, PESEL, data i miejsce urodzenia, adres zamieszkania, adres zameldowania, numer telefonu, e-mail, numer legitymacji szkolnej, wyniki na świadectwie ukończenia gimnazjum, wyniki egzaminu gimnazjalnego, informacje o dysfunkcjach, imiona i nazwiska rodziców/opiekunów, telefon rodziców/opiekunów, e-mail rodziców/opiekunów, zawód rodziców/opiekunów, miejsce pracy rodziców/opiekunów

	Dokumentacja komisji d/s opłat za szkołę (w tym zwolnienia z opłat)	Imię i nazwisko ucznia, imiona i nazwiska rodziców/opiekunów oraz ich adresy zamieszkania, numery telefonów, adresy e-mail, miejsca zatrudnienia, numery PESEL i NIP, opis sytuacji rodzinnej, dane o dochodach rodziny (w tym zasiłkach) – kopie PIT lub rocznego zeznania podatkowego, wysokość przyznanej ulgi, dokumenty potwierdzające rozwód rodziców ucznia
	Księga uczniów	Imiona i nazwisko, data i miejsce urodzenia, PESEL, adres zamieszkania, imiona i nazwiska rodziców/opiekunów, adres zamieszkania rodziców/opiekunów
	Arkusze ocen	Imiona i nazwisko, data i miejsce urodzenia, PESEL, numer w *Księdze uczniów*, adres zamieszkania, imiona i nazwiska rodziców/opiekunów, adres zamieszkania rodziców/opiekunów
	Księga legitymacji	Imię i nazwisko, numer legitymacji
	Rejestr zaświadczeń	Imię i nazwisko, data urodzenia
	Rejestr świadectw ukończenia szkoły i świadectw maturalnych oraz ich duplikatów	Imię i nazwisko, PESEL, numer świadectwa
	Dokumentacja ubezpieczeniowa	Imię i nazwisko, data urodzenia, PESEL, adres zamieszkania, numer telefonu, e-mail, imię i nazwisko rodzica/opiekuna, numer konta rodzica/opiekuna
	Dokumentacja kart rowerowych	Imię i nazwisko, data urodzenia, adres zamieszkania, numer karty

	Dokumentacja udziału w olimpiadach przedmiotowych	Imię i nazwisko, data i miejsce urodzenia
	Karty zdrowia	Imię i nazwisko, data urodzenia, adres zamieszkania, PESEL
	Rejestr opłat za szkołę	Imię i nazwisko płatnika (rodzica/opiekuna), adres, e-mail, numer telefonu

I.4. System przetwarzania danych osobowych

W skład systemu wchodzą:

- dokumentacja papierowa (korespondencja, dokumenty pracowników i uczniów);
- wydruki komputerowe;
- urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji.

I.5. Środki techniczne i organizacyjne stosowane w przetwarzaniu danych osobowych

I.5.1 **Cele polityki bezpieczeństwa**

Polityka bezpieczeństwa informacji Szkoły ma na celu zabezpieczenie przetwarzanych danych osobowych przed ich użyciem w celach innych niż zadania statutowe Szkoły.

I.5.2 **Zasady funkcjonowania polityki bezpieczeństwa**

Realizując Politykę bezpieczeństwa informacji (przetwarzając dane osobowe) Szkoła kieruje się następującymi zasadami:

- zasada merytorycznej poprawności – przetwarzane dane są prawdziwe i aktualizowane;
- zasada legalności – dane są przetwarzane zgodnie z prawem;
- zasada celowości – dane są przetwarzane dla oznaczonych, zgodnych z prawem celów i nie są poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
- zasada poufności danych – dane nie są udostępniane osobom nieupoważnionym;
- zasada adekwatności – przetwarzane są tylko takie dane, które są niezbędne ze względu na działania statutowe Szkoły;
- zasada ograniczenia czasowego – dane w postaci umożliwiającej identyfikację osób, których dotyczą, przechowuje się nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania.

I.5.3 **Osoby odpowiedzialne za bezpieczeństwo danych osobowych**

- **Administrator Danych Osobowych (ADO)** – Dyrektor Szkoły:
  - określa i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych;
  - decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych;
  - odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole.
- **Administrator Bezpieczeństwa Informacji (ABI)** – pracownik Szkoły wyznaczony przez Dyrektora:
  - nadzoruje zgodne z prawem przetwarzanie danych osobowych w Szkole w imieniu ADO;
  - wydaje upoważnienia do przetwarzania danych osobowych, określając w nich zakres i termin ważności;
  - prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;
  - ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych.

I.5.4 **Udzielanie dostępu do danych osobowych**

- Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne, imienne upoważnienie wydane przez ABI;

- Dostęp do danych osobowych może mieć wyłącznie osoba znająca przepisy ustawy o ochronie danych osobowych oraz obowiązującą w Szkole *Politykę bezpieczeństwa* i *Instrukcję zarządzania systemem informatycznym*, co potwierdza w pisemnym oświadczeniu.

I.5.5 **Udostępnianie i powierzanie danych osobowych**

- O udostępnieniu lub powierzeniu danych osobowych decyduje ADO;
- Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą;
- ADO odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób;
- Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:
  - adresat wniosku (administrator danych),
  - wnioskodawca,
  - podstawa prawna (uzasadnienie),
  - wskazanie przeznaczenia,
  - zakres informacji,
  - zobowiązanie do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych;
- Każda osoba fizyczna, której dane przetwarzane są w Szkole, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych a także prawo do kontroli i poprawiania swoich danych osobowych oraz w przypadkach

określonych w art. 32 ust 1 pkt 7 i 8 *Ustawy o ochronie danych osobowych* prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych i przekazywania ich innym podmiotom. Informacji udziela i żądania rozpatruje ABI.

I.5.6 **Bezpieczeństwo przetwarzania danych osobowych w formie tradycyjnej**

- Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych, pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. W czasie nieobecności pracownika pomieszczenie powinno być zamknięte na klucz;

- Kluczami do szaf, w których przechowywane są dane osobowe, dysponują jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych;

- Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

I.5.7 **Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych**

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w *Instrukcji zarządzania systemem informatycznym*

I.6 Analiza ryzyka związanego z przetwarzaniem danych osobowych

I.6.1 **Identyfikacja zagrożeń**

Forma przetwarzania danych osobowych	Zagrożenia
Przetwarzanie tradycyjne	• zdarzenia losowe (zalanie, pożar itp.); • zaniedbanie (niewłaściwe przechowywanie, nieprzestrzeganie zasad *Polityki bezpieczeństwa*); • kradzież.
Przetwarzanie w systemach informatycznych	• zdarzenia losowe (zalanie, pożar itp.); • zaniedbanie (nieprzestrzeganie zasad *Polityki bezpieczeństwa* oraz *Instrukcji zarządzania systemem informatycznym*); • niewłaściwe administrowanie systemem; • włamanie do systemu; • niekontrolowane wytwarzanie i wypływ danych poza obszar

	przetwarzania za pośrednictwem przenośnych nośników informacji; • niekontrolowana obecność osób nieuprawnionych w miejscu przetwarzania danych; • uszkodzenie systemu.

I.6.2 **Sposób zabezpieczenia danych**

Forma przetwarzania danych osobowych	Sposoby ochrony
Przetwarzanie tradycyjne	• ochrona budynku przez całą dobę przez strażnika/portiera; • zapoznanie pracowników Szkoły z *Polityką bezpieczeństwa* i *Instrukcją zarządzania systemem informatycznym* oraz zobowiązanie ich do przestrzegania zawartych w nich procedur; • przetwarzanie danych wyłącznie przez osoby upoważnione przez ABI; • przechowywanie danych w zamykanych na klucz pomieszczeniach; • przechowywanie danych w zamykanych na klucz szafach; • dysponowanie kluczami do szaf i pomieszczeń, w których są przetwarzane dane, wyłącznie przez osoby upoważnione.
Przetwarzanie w systemach informatycznych	• ochrona budynku przez całą dobę przez strażnika/portiera; • zapoznanie pracowników Szkoły z *Polityką bezpieczeństwa* i *Instrukcją zarządzania systemem informatycznym* oraz zobowiązanie ich do przestrzegania zawartych w nich procedur; • przetwarzanie danych wyłącznie przez osoby upoważnione przez ABI; • stosowanie regularnie aktualizowanych programów antywirusowych; • przydzielenie użytkownikom systemu indywidualnych kont wraz z

	chroniącymi je loginami i hasłami; • zabezpieczenie pomieszczenia serwerowni przed dostępem osób nieupoważnionych.

I.6.3 **Określenie wielkości ryzyka naruszenia bezpieczeństwa danych**

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka.

I.6.4 **Identyfikacja obszarów wymagających szczególnych zabezpieczeń**

ABI przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawia Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych i organizacyjnych niezbędnych dla zapewnienia właściwej ochrony przetwarzanych danych.

II INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

II.1 Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym

- Dane osobowe w systemach informatycznych mogą być przetwarzane tylko przez osoby posiadające do tego pisemne upoważnienie wydane przez ABI.

- Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada firma świadcząca usługi informatyczne dla Szkoły zgodnie z zawartą umową.

- Firma świadcząca usługi informatyczne dla szkoły nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia wydanego przez ABI.

II.2 Zabezpieczenie danych w systemie informatycznym

- Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system uprawnień i system kont zabezpieczonych hasłami .

- Hasło nie może być udostępniane osobom nieuprawnionym ani zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

- System jest zabezpieczony aktywną ochroną antywirusową.

II.3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym

- Po zakończeniu pracy oraz wtedy, gdy praca zostaje chwilowo przerwana a użytkownik odchodzi od komputera, należy wylogować się z systemu.

- W przypadku planowego zawieszenia korzystania z systemu informatycznego (konserwacja sprzętu lub inne czynności) należy poinformować o tym użytkowników na co najmniej jedną dobę przed planowanym zawieszeniem.

- W razie podejrzenia, że bezpieczeństwo systemu zostało zagrożone, użytkownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ABI lub ADO.

II.4 Udostępnianie danych

Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.

II.5 Przeglądy i konserwacja systemu

- Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych wykonawców.

- Prace wymienione powyżej powinny być prowadzone w sposób uniemożliwiający osobom nieupoważnionym dostęp do danych.

II.6 Niszczenie wydruków i nośników danych

- Wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach, i po upływie ich przydatności są niszczone przy użyciu niszczarki.

- Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

- Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć.

III. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH OSOBOWYCH

III.1 Istota naruszenia danych osobowych

Naruszeniem danych osobowych jest każde stwierdzone:

- nieuprawnione ujawnienie danych osobowych;
- udostępnienie ich lub umożliwienie dostępu do nich osobom nieupoważnionym;
- przejęcie danych przez osobę nieupoważnioną;
- nieautoryzowany dostęp do danych;
- nieautoryzowane modyfikacje lub zniszczenie danych;
- udostępnienie danych nieautoryzowanym podmiotom;
- pozyskiwanie danych z nielegalnych źródeł.

III.2 Postępowanie w przypadku naruszenia bezpieczeństwa danych osobowych

- Użytkownik systemu, który stwierdzi naruszenie bezpieczeństwa danych, jest zobowiązany niezwłocznie zgłosić to ABI lub ADO.

- ABI lub ADO zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania.

- ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych, sporządzając raport, który przekazuje ADO.

- ABI zasięga potrzebnych opinii i proponuje działania naprawcze.

III.3 Sankcje

- Wobec osoby, która naruszyła bezpieczeństwo danych osobowych, wszczyna się postępowanie dyscyplinarne.

- Wobec osoby, która będąc świadoma naruszenia bezpieczeństwa danych osobowych, nie podjęła działania określonego w niniejszym dokumencie, wszczyna się postępowanie dyscyplinarne.

- Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załącznik nr 1.

.....
(pieczęć szkoły)

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 37 *Ustawy o ochronie danych osobowych* z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.) upoważniam Panią/Pana .....
zatrudnioną/ego w I Społecznym Liceum Ogólnokształcącym im. Maharadży Jam Saheba Digvijay Sinhji 01-167 Warszawa, ul. Zawiszy 13 na stanowisku.....
do przetwarzania danych osobowych zawartych w zbiorach danych Szkoły.

Upoważnienie dotyczy przetwarzania danych osobowych w sposób potrzebny do wypełnienia obowiązków służbowych i w zakresie wymaganym przez te obowiązki.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z niniejszym dokumentem oraz przepisami określonymi w *Ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r.* (Dz. U. z 2002 r. Nr 101 poz. 926 z późniejszymi zmianami) i towarzyszących jej aktach wykonawczych a także z wewnętrzną *Polityką bezpieczeństwa informacji* i *Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* w I Społecznym Liceum Ogólnokształcącym im. Maharadży Jam Saheba Digvijay Sinhji w Warszawie.

Wymieniona w *Upoważnieniu* osoba zostaje wpisana do *Ewidencji osób upoważnionych do przetwarzania danych osobowych znajdujących się w zbiorach danych Szkoły*.

Upoważnienie jest ważne do odwołania lub ustania zatrudnienia w Szkole.

....
(Data i podpis upoważniającego (ABI)) (Data i podpis osoby upoważnionej)

Rozdzielnik: 1 egz. dla upoważnionego, 1 egz. do dokumentacji

Załącznik nr 2

Oświadczenie osoby upoważnionej do przetwarzania danych osobowych

Oświadczam, że zapoznałem/-am się z przepisami prawa dotyczącymi ochrony danych osobowych oraz z obowiązującymi w I Społecznym Liceum Ogólnokształcącym im. Maharadży Jam Saheba Digvijay Sinhji w Warszawie dokumentami: *Polityką bezpieczeństwa informacji* i *Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.* Przyjmuję do wiadomości zawarte w nich przepisy i zobowiązuję się do ich przestrzegania.

Zobowiązuję się do zachowania poufności danych osobowych zawartych w zbiorach danych Szkoły i zachowania tajemnicy o sposobach ich zabezpieczenia także po odwołaniu upoważnienia i po ustaniu zatrudnienia.

.....
(Data i czytelny podpis osoby upoważnionej)

Rozdzielnik: 1 egz. dla upoważnionego, 1 egz. do dokumentacji

Załącznik nr 3

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator osoby upoważnionej*	Nazwy zbiorów danych objętych upoważnieniem
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					

.....
pieczęć i podpis dyrektora Szkoły (ADO)