

ZARZĄDZENIE Nr 357/18
Dyrektora II Społecznego Liceum Ogólnokształcącego
im. Toniego Halika w Ostrołęce
z dnia 15.05.2018r.

**w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji zarządzania systemem
przetwarzania danych osobowych przy użyciu systemu informatycznego
i w sposób ręczny w II Społecznym Liceum Ogólnokształcącym im. Toniego Halika w
Ostrołęce**

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922. z późn. zm.) oraz § 3 i 4 Rozporządzenia 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).

Zarządza się, co następuje:

§ 1.

Wprowadzam w II Społecznym Liceum Ogólnokształcącym im. Toniego Halika w Ostrołęce Politykę Bezpieczeństwa, której treść stanowi załącznik nr 1 do zarządzenia, oraz Instrukcję zarządzania systemem informatycznym przetwarzania danych osobowych przy użyciu systemu informatycznego i w sposób ręczny, która stanowi załącznik nr 2 do zarządzenia.

§ 2.

Każdy pracownik dopuszczony do przetwarzania danych osobowych jest obowiązany zapoznać się z treścią załącznika nr 1 i nr 2 do zarządzenia lub wybranym zakresem odpowiednim do wydanego upoważnienia.

§ 3.

Oświadczenie o zapoznaniu się z treścią powyższych załączników zaopatrzone w podpis pracownika i datę, dołącza się do akt osobowych.

§ 4.

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa oraz stosowania w pracy Instrukcji Zarządzania Systemem Informatycznym pod sankcją konsekwencji służbowych, przewidzianych prawem.

§ 5.

Zarządzenie wchodzi w życie z dniem ogłoszenia.

Załącznik 1 do Zarządzenia Nr357/18
Dyrektora II Społecznego Liceum Ogólnokształcącego
im. Toniego Halika w Ostrołęce

**POLITYKA BEZPIECZEŃSTWA W ZAKRESIE ZARZĄDZANIA PRZETWARZANIEM DANYCH
OSOBOWYCH
w II Społecznym Liceum Ogólnokształcącym
im. Toniego Halika w Ostrołęce**

Zatwierdzam
Dyrektor II Społecznego Liceum
Ogólnokształcącego im. Toniego
Halika w Ostrołęce

I. POSTANOWIENIA WSTĘPNE

1. Polityka bezpieczeństwa w zakresie zarządzania przetwarzaniem danych osobowych, w II Społecznym Liceum Ogólnokształcącym im. Toniego Halika w Ostrołęce, jest dokumentem zwanym dalej polityką bezpieczeństwa, który określa zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym ujawnieniem.

2. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

3. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zawiera:

- 1) identyfikację zasobów systemu tradycyjnego i informatycznego;
- 2) wykaz pomieszczeń, tworzący obszar, w którym przetwarzane są dane osobowe;
- 3) wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych;
- 4) opis struktury zbiorów danych i sposoby ich przepływu;
- 5) środki techniczne i organizacyjne, służące zapewnieniu poufności przetwarzanych danych.

4. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w II Społecznym Liceum Ogólnokształcącym w Ostrołęce jak i innych, np. studentów, osób odbywających praktyki pedagogiczne, innych osób wykonujących prace na terenie szkoły.

II. DEFINICJE

Definicje:

Ilekoć w instrukcji jest mowa o:

administratorze danych osobowych – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W II Społecznym Liceum Ogólnokształcącym im. Toniego Halika w Ostrołęce funkcję administratora danych pełni dyrektor szkoły;

administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji (ABI) a od 25 maja 2018r. ABI staje się Inspektorem Ochrony Danych Osobowych (**IODO**); II Społeczne Liceum Ogólnokształcące im. Toniego Halika w Ostrołęce jako szkoła niepubliczna nie ma obowiązku zatrudniania IODO;

administratorze systemu informatycznego – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagane specjalnych uprawnień;

dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg. określonych kryteriów oraz celów;

przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;

hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to pracownika szkoły, która upoważniona została do przetwarzania danych osobowych przez dyrektora szkoły na piśmie;

poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

rozporządzeniu MSWiA – rozumie się przez to rozporządzenie 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.);

serwisancie – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;

sieci publicznej – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

szkole – rozumie się przez to **II Społeczne Liceum Ogólnokształcące im. Toniego Halika w Ostrołęce**

teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922. z późn. zm.);

uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

użytkownika – rozumie się przez to pracownika szkoły upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło w przypadku korzystania z systemu informatycznego.

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych osobowych.

Funkcję administratora danych osobowych sprawuje dyrektor szkoły. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

- 1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,
- 2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, oraz odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,
- 3) wyznacza administratora bezpieczeństwa informacji oraz administratora sieci oraz określa zakres ich zadań i czynności,
- 4) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą dokumentację z zakresu ochrony danych, o ile jako właściwą do jej prowadzenia nie wskaże inną osobę,
- 5) zapewnia użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,
- 6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur.

Administrator danych osobowych ma prawo:

- 1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej szkole;
- 2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzanie niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
- 3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
- 4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
- 5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.

3. Administrator systemu informatycznego

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

- 1) zarządza systemem informatycznym, w którym są przetwarzane dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
- 2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
- 3) na wniosek dyrektora szkoły przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;
- 4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
- 5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
- 6) wyrejestrowuje użytkowników na polecenie administratora danych;
- 7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych;
- 8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora bezpieczeństwa informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;
- 9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
- 10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
- 11) podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Osoba upoważniona do przetwarzania danych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

- 1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie

stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;

4) stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

5) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcji obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. IDENTYFIKACJA ZASOBÓW SYSTEMU INFORMATYCZNEGO

1. Struktura informatyczna **w II Społecznym Liceum Ogólnokształcącym im. Toniego Halika w Ostrołęce** składa się z:

1) sieci wewnętrznej, mieszczącej się w pomieszczeniach szkoły i jest połączona siecią zbudowaną w oparciu o łącza dzierżawione w Orange Polska S.A. Al. Jerozolimskie 160, 02-360 Warszawa (Neostrada).

Informacje przetwarzane w tej strukturze są jawne, ale podlegają ochronie zgodnie z przepisami ustawy.

V. WYKAZ POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji nadanych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.

2. Dane osobowe przetwarzane są na terenie szkoły przy ul. Gen. Ignacego Prądzyńskiego 5 w Ostrołęce.

3. Ze względu na nagromadzenie danych osobowych szczególnie chronione powinny być pomieszczenia, zgodnie z poniższym wykazem.

Budynek	Rodzaj dokumentów	Miejsce przechowywania
Budynek szkolny II SLO przy ul.Prądyńskiego 5 w Ostrołęce	Dzienniki lekcyjne	Pokój nauczycielski – klucze dostępne w kancelarii szkoły
	Dzienniki zajęć pozalekcyjnych	Pokój nauczycielski – klucze dostępne w kancelarii szkoły
	Dzienniki zajęć specjalistycznych	Pokój nauczycielski – klucze dostępne w kancelarii szkoły
	Dziennik pedagoga szkolnego, opinie i orzeczenia z Poradni Psychologiczno - Pedagogicznej	Pokój pedagoga (biblioteka) I.piętro budynku szkolnego – klucze dostępne w kancelarii szkolnej i pokoju nauczycielskim
	Dziennik bibliotekarza	Pokój pedagoga (biblioteka) I.pietro budynku szkolnego – klucze dostępne w kancelarii szkolnej i pokoju nauczycielskim
	Księga ewidencji uczniów	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczk
	Arkusze ocen, księgi arkuszy ocen absolwentów	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątaj
	Dokumentacja rekrutacyjna uczniów	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątaj
	Dokumenty nadzoru pedagogicznego	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątaj
	Protokoły Rady Pedagogicznej	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątaj
	Ewidencja i deklaracje uczniów przystępujących do egzaminu maturalnego	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątaj
	Arkusze organizacyjny szkoły	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątaj

Ewidencja legitymacji szkolnych, wydawanych zaświadczeń uczniom	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
Ewidencja świadectw ukończenia szkoły oraz maturalnych	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
Wnioski rodziców dotyczące nauki religii i WDŻ	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
Zwolnienia lekarskie uczniów z wychowania fizycznego i taktyki i technik interwencji	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
SIO – System Informacji Oświatowej	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
Książka kontroli zewnętrznych	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątająca
Lista obecności pracowników	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
Dziennik korespondencji	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
Rejestr upoważnień	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię)- klucze mają dyrektor szkoły, główny księgowy, osoba sprzątająca
Akta osobowe	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię)- klucze mają dyrektor szkoły, główny księgowy, osoba sprzątająca
Listy płac i karty wynagrodzeń	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, osoba sprzątająca
Dokumentacja kadrowa (umowy o pracę, cywilnoprawne, rozliczenia godzin ponadwymiarowych, listy obecności, zwolnienia lekarskie	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką

	pracowników i karty zasiłkowe).	
	Dokumentacja księgowa	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
	Dokumentacja ubezpieczeniowa uczniów NW	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
	Dokumentacja ubezpieczeniowa pracowników (dobrowolne ubezpieczenie grupowe)	Gabinet dyrektora szkoły (parter budynku szkolnego, wejście przez kancelarię) – klucze mają dyrektor, główny księgowy, osoba sprzątająca
	Dokumentacja Ogólnopolskiej Olimpiady Wiedzy o Prawie	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
	Dokumentacja Małej Olimpiady Matematyczno – Fizycznej	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
	CCTV monitoring wizyjny	Kancelaria szkolna (parter budynku szkolnego) – klucze mają dyrektor szkoły, główna księgowa, sprzątaczką
	Dokumenty archiwalne	Archiwum szkolne – klucze w kancelarii szkolnej

Opis pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe

1. II Społeczne Liceum Ogólnokształcące im. Toniego Halika w Ostrołęce mieści się w budynku przy ulicy Gen. Ignacego Prądzyńskiego 5 w Ostrołęce, są tu: kancelaria szkolna, pokój dyrektora, pokój nauczycielski, pokój pedagoga szkolnego (jednocześnie biblioteka) oraz archiwum.
2. Kancelaria i pokój dyrektora znajdują się na parterze i do gabinetu dyrektora szkoły wchodzi się przez kancelarię szkolną. Dyrektor szkoły zajmuje gabinet dyrektora a kancelarię główna księgowa szkoły. W pokojach tych przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. płyty CD przechowuje się w szafach zamykanych na klucze, które są w posiadaniu dyrektora i głównej księgowej. W komputerze głównej księgowej znajdują się: program SIO – system informacji oświatowej, listy płac pracowników oraz Płatnik – program do rozliczania i przesyłania deklaracji ZUS pracowników. Programy może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł. W komputerze dyrektora szkoły znajdują się: program HERMES do przesyłania informacji z deklaracji maturalnych uczniów.
3. Pokój nauczycielski znajduje się na parterze budynku szkolnego. W pokoju tym przetwarzane są dane osobowe uczniów i ich rodziców ręcznie oraz elektronicznie (laptop do korzystania z dziennika elektronicznego). Dokumentację papierową przechowuje się podczas zajęć dydaktycznych w szafach z przegródkami w pokoju

nauczycielskim, na okres przerw i ferii są zamykane w szafie w kancelarii szkolnej. Do dziennika elektronicznego mogą się logować tylko uprawnieni nauczyciele i pracownicy za pomocą swojego loginu i hasła.

4. Pokój pedagoga szkolnego znajduje się na parterze budynku IISLO i przystosowany jest do pracy dla dwóch osób. W pokoju tym przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. płyty CD przechowuje się w szafie zamykanej na klucz, które są w posiadaniu pedagoga i kancelarii szkolnej. Komputer może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
5. Biblioteka szkolna znajduje się na parterze budynku II SLO.
6. Pieczęcie z nazwą i siedzibą instytucji oraz imienne są przechowywane w szafie pancerniej które otwiera i zamyka główna księgowa szkoły lub dyrektor.
7. Przesyłki zawierające dane osobowe przesyła się jako polecone z ewentualnym zwrotnym potwierdzeniem odbioru oraz zabezpieczone w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby nieupoważnione.
8. Dokumenty zawierające dane osobowe przekazuje się do archiwum mieszczącego się W II SLO, po okresie przydatności dokumenty zawierające dane osobowe niszczy się na podstawie decyzji dyrektora komisyjnie, w warunkach gwarantujących zabezpieczenie danych osobowych w sposób gwarantujący uniemożliwienie ich odtworzenia, wykazy i spisy zdawczo - odbiorcze dokumentów zawierające dane osobowe przekazywanych do archiwum oraz protokoły zniszczenia dokumentów przechowuje administrator danych. Dostęp do archiwum szkolnego posiada główna księgowa oraz dyrektor szkoły.
9. Dokumenty zawierające dane osobowe niezbędne do pracy w terenie należy przechowywać w warunkach gwarantujących ich należytą ochronę.

VI. WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMÓW STOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania danych/ nazwa zasobu danych	Lokalizacja zbioru/ zasobu	Miejsce przetwarzania danych
1.	Kandydaci do szkoły	WINDOWS 7, WINDOWS 10	Kancelaria szkolna, gabinet dyrektora	Kancelaria szkolna, gabinet dyrektora
		CCTV – monitoring na korytarzach szkolnych i budynku szkolnym	Kancelaria szkolna	Kancelaria szkolna
2.	Uczniowie szkoły	Księga uczniów	Kancelaria szkolna	Kancelaria szkolna
		Dzienniki lekcyjne papierowe	Pokój nauczycielski	Sale lekcyjne, pokój nauczycielski
		Dziennik elektroniczny	Pokój nauczycielski, gabinet dyrektora, kancelaria szkoły	Pokój nauczycielski, gabinet dyrektora, kancelaria szkoły
		Arkusze ocen	Gabinet dyrektora	Pokój nauczycielski

		SIO	Kancelaria szkoły, gabinet dyrektora szkoły	Kancelaria szkoły, gabinet dyrektora szkoły
		Dokumentacja pedagoga szkolnego	Pokój pedagoga szkolnego	Pokój pedagoga szkolnego, pokój nauczycielski
		Dokumentacja wychowawcy klasy	Pokój nauczycielski	Pokój nauczycielski
		HERMES, planer.edu.pl	Gabinet dyrektora szkoły	Gabinet dyrektora szkoły
		CCTV	Teren przed budynkiem szkolnym (parking i działka szkolna), korytarze szkolne, sala gimnastyczna (nr20), pracownia informatyczna (nr14), pracownia językowa (nr15), aula.	Kancelaria szkolna
3.	Pracownicy szkoły	Akta osobowe	Gabinet dyrektora szkoły	Gabinet dyrektora szkoły, kancelaria szkoły
		SIO	Gabinet dyrektora szkoły, kancelaria szkoły	Gabinet dyrektora szkoły, kancelaria szkoły
		Edytor tekstu	Gabinet dyrektora szkoły, kancelaria szkoły	Gabinet dyrektora szkoły, kancelaria szkoły
		CCTV	Teren przed budynkiem szkolnym (parking i działka szkolna), korytarze szkolne, sala gimnastyczna (nr20), pracownia informatyczna (nr14), pracownia językowa (nr15), aula.	Kancelaria szkolna
4.	Księgowość – finanse szkoły	PŁATNIK ZUS	Kancelaria szkoły	Kancelaria szkoły
		Listy płac	Kancelaria szkoły	Kancelaria szkoły
		Arkusz kalkulacyjny	Kancelaria szkoły	Kancelaria szkoły
5.	Uczestnicy Ogólnopolskiej	Edytor tekstu i arkusz kalkulacyjny	Kancelaria szkoły	Kancelaria szkoły

	Olimpiady Wiedzy o Prawie organizowanej przez II SLO	CCTV	Teren przed budynkiem szkolnym (parking i działka szkolna), korytarze szkolne, aula.	Kancelaria szkolna
6.	Uczestnicy Małej Olimpiady Matematyczno – Fizyczna	Edytor tekstu i arkusz kalkulacyjny	Kancelaria szkoły	Kancelaria szkolna
		CCTV	Teren przed budynkiem szkolnym (parking i działka szkolna), korytarze szkolne, aula.	Kancelaria szkolna

WYKAZ PROGRAMÓW STOSOWANYCH W SZKOLE:

- WINDOWS 7
- WINDOWS 10
- HERMES, platforma planer.edu.pl
- SIO – system informacji oświatowej
- CCTV – monitoring wizyjny
- PŁATNIK – program do przesyłania i rozliczania deklaracji ZUS
- MS Office 2007

VII. STRUKTURA ZBIORÓW DANYCH, SPOSÓB PRZEPŁYWU DANYCH I ZAKRES ICH PRZETWARZANIA

KARTY ZBIORÓW

Lp.	Nazwa zbioru danych	Podstawa prawna upoważniająca do prowadzenia zbioru danych	Struktura zbioru	Program	Dostęp
1.	Kandydaci do szkoły	Ustawa z dn.14 grudnia 2016r. Prawo oświatowe ze zm.; ustawa z dn.29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Imię i nazwisko, PESEL, data i miejsce urodzenia, miejsce zamieszkania, imiona i nazwiska rodziców wraz z adresami zamieszkania, telefony kontaktowe kandydata i rodziców/ opiekunów prawnych, informacja o stanie zdrowia, wyznaniu (deklaracja o uczestnictwie w religii, wdż)	Edytor tekstu	Dyrektor szkoły, główna księgowa
2.	Księga uczniów	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumentacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumentacji.	Nazwiska i imiona uczniów, data i miejsce urodzenia, PESEL, miejsce zamieszkania nazwiska i imiona rodziców z miejscem ich zamieszkania		Dyrektor szkoły, główna księgowa
3.	dzienniki lekcyjne	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumentacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumentacji.	Nazwiska i imiona uczniów, data i miejsce urodzenia, PESEL, miejsce zamieszkania nazwiska i imiona rodziców z telefonami kontaktowymi, oceny uczniów, usprawiedliwienia nieobecności, uwagi co do zachowania i pochwały ucznia, nazwiska i imiona nauczycieli	Dziennik elektroniczny blizejszkoły.pl	Dyrektor szkoły, główna księgowa, pedagog szkolny, nauczyciele

4.	Arkusze ocen uczniów	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumentacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumentacji.	Nazwiska i imiona uczniów, data i miejsce urodzenia, PESEL, adres zamieszkania, imiona i nazwiska rodziców, nr księgi ucznia, klasa, zawód/ profil, wyniki klasyfikacji rocznej, data ukończenia nauki.	Dziennik elektroniczny blizejszkoły.pl	Dyrektor szkoły, główna księgowa, pedagog szkolny, nauczyciele
5.	Księgi arkuszy ocen absolwentów	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumentacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumentacji.	Nazwiska i imiona uczniów, data i miejsce urodzenia, PESEL, adres zamieszkania, imiona i nazwiska rodziców, nr księgi ucznia, klasa, zawód/ profil, wyniki klasyfikacji rocznej, data ukończenia nauki.		Dyrektor szkoły
6.	Ewidencja legitymacji szkolnych	Ustawa z dn.29 sierpnia 1997r. O ochronie danych osobowych; rozporządzenie MEN z dn. 18 stycznia 2017r. ws. świadectw, dyplomów państwowych i innych druków szkolnych.	Nazwisko i imię ucznia, nr legitymacji, data wystawienia, klasa, podpis ucznia		Dyrektor szkoły, główna księgowa
7.	Ewidencja świadectw ukończenia szkoły i maturalnych	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	nazwisko i imię ucznia, nr świadectwa maturalnego, podpis ucznia, upoważnienia notarialne do odebrania świadectwa		Dyrektor szkoły

8.	Protokoły Rady Pedagogicznej	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe ze zm.; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumnetacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumnetacji.	nazwiska i imiona uczniów, ich wyniki w nauczaniu, nazwiska i imiona nauczycieli,	Edytor tekstu	Dyrektor szkoły, nauczyciele
9.	deklaracje maturalne	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwiska i imiona uczniów, PESEL, miejsce zamieszkania, telefony kontaktowe i adresy email, informacje o dostosowanie ze względu na stan zdrowia	HERMES, planer.edu.pl	Dyrektor szkoły, pedagog szkolny
10.	karty biblioteczne	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.,ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe ze zm.	Nazwiko i imię, klasa, wypozyczenia		Dyrektor szkoły, bibliotekarz
11.	Dziennik Pedagoga Szkolnego	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumnetacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumnetacji.	Nazwiska i imiona uczniów, PESEL, nazwiska i imiona rodziców, adresy zamieszkania, stan zdrowia, orzeczenia z PPP		Dyrektor szkoły, pedagog szkolny

12.	dokumentacja wycieczek szkolnych - listy uczniów	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.; rozporządzenie MENiS z dn. 08 listopada 2001r. Ws.warunków i sposobu organizowania przez publiczne przedszkola, szkoły i placówki krajoznawstwa i turystyki ze zm.	Nazwiko i imię, PESEL, nr legitymacji szkolnej, adres zamieszkania, Nazwiska i imiona rodziców, telefony kontaktowe do rodziców, miejsce i czas trwania wycieczki, informacje o stanie zdrowia	Edytor tekstu, arkusz kalkulacyjny	Dyrektor szkoły, główna księgowa, nauczyciele
13.	ubezpieczenie uczniów NW	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe ze zm.; rozporządzenie MENiS z dn.31 grudnia 2002r. Ws.bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach ze zm.	Nazwisko i imię ucznia, PESEL, adres zamieszkania, klasa, nazwa i dane rejestracyjne zakładu ubezpieczeń	Edytor tekstu	Dyrektor szkoły, główna księgowa
14.	Opinie i orzeczenia z Poradni Psychologiczno - Pegagogicznej	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumnetacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumnetacji.	Nazwiska i imiona, PESEL, adres zamieszkania ucznia, nazwiska imiona rodziców, sytuacja rodzinna, stan zdrowia, zalecenia dla nauczycieli i rodziców		Dyrektor szkoły, pedagog szkolny
15.	Wnioski rodziców dotyczące nauki religii i WDŻ	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwiska i imiona ucznia, adres zamieszkania, nazwiska i imiona rodziców, PESEL ucznia, klasa, ewentualnie wyznanie		Dyrektor szkoły, główna księgowa, nauczyciele
16.	Zwolnienia lekarskie uczniów z wychowania fizycznego i taktyki i technik interwencji	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwiska i imiona ucznia, adres zamieszkania, nazwiska i imiona rodziców, PESEL ucznia, klasa, stan zdrowia, zwolnienie lekarskie	Edytor tekstu	Dyrektor szkoły, główna księgowa, nauczyciele

17.	Dzienniki zajęć pozalekcyjnych	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 16 grudnia 2016r. Prawo Oświatowe; rozporządzenie MEN z dn.29 sierpnia 2014r. Ws. Prowadzenia przez publiczne przedszkola, szkoły, placówki dokumentacji przebiegu nauczania, działalności wychowawczej i piekuńczej oraz rodzajów tej dokumentacji.	Nazwiska i imiona uczniów, data i miejsce urodzenia, PESEL, miejsce zamieszkania nazwiska i imiona rodziców z telefonami kontaktowymi, oceny uczniów, usprawiedliwienia nieobecności, uwagi co do zachowania i pochwały ucznia, nazwiska i imiona nauczycieli		Dyrektor szkoły, nauczyciele, pedagog szkolny
18.	zgody na przetwarzanie danych osobowych	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwisko i imiona pracowników, adres zamieszkania, podpis		Dyrektor szkoły
19.	akta osobowe pracowników	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 26 stycznia 1982r. Karta Nauczyciela, ustawa z dn.26 czerwca 1974r. Kodeks Pracy; rozporządzenie MPiPS z dn. 28 maja 1996r. W spr. zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika	Nazwisko i imię, PESEL, NIP, nazwisko rodowe, data i miejsce urodzenia, adres zamieszkania, dowód osobisty, imię i nazwisko ojca i matki, nazwisko rodowe matki, stan cywilny, rodzinny, wykształcenie, nazwa i rok ukończenia szkoły, uczelni, nr rachunku bankowego, warunki pracy, staz pracy, nagrody, kary, zawód wyuczony, wykonywany, kwalifikacje, uprawnienia, stan zdrowia, informacje z Krajowego rejestru Karnego, nieobecności w pracy		Dyrektor szkoły, główna księgowa

20.	Rekrutacja pracowników	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 26 stycznia 1982r. Karta Nauczyciela, ustawa z dn.26 czerwca 1974r. Kodeks Pracy; rozporządzenie MPiPS z dn. 28 maja 1996r. W spr. zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika	Nazwisko i imie, PESEL, data i miejsce urodzenia, adres zamieszkania, wykształcenie, staz pracy		Dyrektor szkoły
21.	System Informacji Oświatowej	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm., ustawa z dn. 15 kwietnia 2011r. O systemie ustawy oświatowej ze zm., rozporządzenie MEN z dn. 09 sierpnia 2012r. W spr.szczegółowego zakresu danych gromadzonych w bazach danych oświatowych, zakresu danych identyfikujących podmioty prowadzące bazy danych oświatowych, terminów przekazywania danych między bazami danych oświatowych oraz wzorów wydruków zestawień zbiorczych ze zm.	Nazwiska i imiona uczniów, miejsce zamieszkania, PESEL, klasa, rozpoczęcie i ukończenie nauki, nazwiska i imiona, PESEL pracowników pedagogicznych, wykształcenie, staz pracy, stopień awansu zawodowego, wymiar zatrudnienia	SIO – system informacji oświatowej	Dyrektor szkoły, główna księgowa
22.	Dobrowolne ubezpieczenie pracowników	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.; zgody ubezpieczonych	Nazwiska i imiona, PESEL pracowników, adres zamieszkania, tel.kontaktowy, stan zdrowia nazwiska i imiona osób uposażonych	PZU ERU	Dyrektor szkoły, główna księgowa
23.	Listy płac pracowników, karty płac	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwiska i imiona,PESEL, adres zamieszkania, data i miejsce urodzenia, składniki i wysokość wynagrodzenia	Arkusz kalkulacyjny, PŁATNIK	Dyrektor szkoły, główna księgowa

24.	Akta księgowe - umowy o pracę, umowy zlecenia, o dzieło	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwiska i imiona, PESEL, adres zamieszkania, data i miejsce urodzenia, składniki i wysokość wynagrodzenia, forma zatrudnienia, okres zatrudnienia	Arkusz kalkulacyjny	Dyrektor szkoły, główna księgowa
25.	Dowody i dokumenty księgowe	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	nazwa, adres, dane rejestracyjne kontrahenta, kwota	Arkusz kalkulacyjny	Dyrektor szkoły, główna księgowa
26.	Dokumentacja podatkowa	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwiska i imię, PESEL, adres zamieszkania, przychód roczny	Arkusz kalkulacyjny	Dyrektor szkoły, główna księgowa
27.	Rozliczenia godzin ponadwymiarowych	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.; ustawa z dn. 26 stycznia 1982r. Karta Nauczyciela ze zm.	Nazwisko i imię, wymiar czasu pracy, wysokość wynagrodzenia, stawka wynagrodzenia	Edytor tekstu, arkusz kalkulacyjny	Dyrektor szkoły, główna księgowa
28.	Rejestr wydanych zaświadczeń dla uczniów	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwisko i imię ucznia, PESEL, adres zamieszkania, klasa, nazwa organu, do którego będzie składane zaświadczenie		Dyrektor szkoły, główna księgowa
29.	Dziennik korespondencji - rejestr pism wychodzących	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm. rozporządzenie Prezesa Rady Ministrów z dn. 18 stycznia 2011r. w spr. instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych	Nazwisko, imię, nazwa instytucji, firmy, adres, email, przedmiot sprawy, data i numer pisma		Dyrektor szkoły, główna księgowa
30.	Awans zawodowy nauczycieli	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.; ustawa 26 stycznia 1982r. Karta Nauczyciela ze zm.	Nazwiska i imiona, data i miejsce urodzenia, miejsce zamieszkania, staż pracy, przebieg zatrudnienia, wykształcenie, tytuł zawodowy	Edytor tekstu	Dyrektor szkoły
31.	Listy obecności pracowników administracji i obsługi	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwisko, imię, zajmowane stanowisko, podpis		Dyrektor szkoły, główna księgowa

32.	Arkusze organizacyjny	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm., rozporządzenie MEN z dn. 21 maja 2001r. W sprawie ramowych statutow publicznego przedszkola oraz publicznych szkół ze zm.	Nazwiska, imiona, wykształcenie, tytuł zawodowy, staż pracy		Dyrektor szkoły
33.	Wykaz zwolnień lekarskich i kart zasiłkowych pracowników	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.; ustawa z dn. 26 czerwca 1997r. Kodeks Pracy ze zm.	Nazwiska, imiona, PESEL, adres zamieszkania, NIP zakładu pracy czas nieobecności, stan zdrowia		Dyrektor szkoły, główna księgowa
34.	Książka kontroli	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm. Akty prawne regulujące proces kontrolny instytucji/ organu przeprowadzającego kontrole	Nazwisko, imię, zakres kontroli		Dyrektor szkoły
35.	Umowy o współpracy	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych; ustawa z dn. 23 kwietnia 1964r. Kodeks Cywilny ze zm.	Nazwa firmy, imię i nazwisko osoby do kontaktu, dane rejestracyjne, NIP, adres, email, telefon, przedmiot umowy		Dyrektor szkoły, główna księgowa
36.	Dokumentacja Ogólnopolskiej Olimpiady Wiedzy o Prawie	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwisko i imiona, PESEL, adres zamieszkania, telefon kontaktowy adres szkoły, data i miejsce urodzenia uczestnika, nazwisko i imię, telefon kontaktowy opiekuna, punktacja uczestnika w poszczególnych etapach, informacja o orzeczeniach Z PPP		Dyrektor szkoły, główna księgowa
37.	Dokumentacja Małej Olimpiady Matematyczno - Fizycznej	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	Nazwisko i imiona uczestnika, szkoła, klasa, nazwisko i imię opiekuna, telefony kontaktowe		Dyrektor szkoły, główna księgowa, nauczyciele
38.	CCTV monitoring wizyjny	Ustawa z dn. 29 sierpnia 1997r. O ochronie danych osobowych ze zm.	wizerunek		Dyrektor szkoły, główna księgowa

VIII. ŚRODKI TECHNICZNE I ORGANIZACYJNE, SŁUŻĄCE ZAPEWNIENIU POUFNOŚCI PRZETWARZANIA DANYCH

1. Bezpieczeństwo osobowe.

Zachowanie poufności.

1. Dyrektor szkoły przeprowadza nabór na wolne stanowiska w drodze oferty. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
2. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia szkolne), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń – zakres obowiązków pracownika.
3. Ryzyko ze strony osób, które dokonują bieżących napraw komputera, minimalizowane jest obecnością użytkownika systemu.

Szkolenia w zakresie ochrony danych osobowych.

1. Administrator bezpieczeństwa informacji uwzględnia następujący plan szkoleń:
 - a) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
 - b) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
 - c) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.
2. Tematyka szkoleń obejmuje:
 - a) przepisy i procedury, dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
 - b) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
 - c) obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
 - d) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
 - e) zasady i procedury określone w polityce bezpieczeństwa.

Strefy bezpieczeństwa.

Do strefy I wchodzi: gabinet dyrektora, kancelaria szkolna. W tej strefie może przebywać dyrektor szkoły, główny księgowy, inni użytkownicy tylko w towarzystwie wymienionych osób funkcyjnych.

Do strefy II wchodzi: pokój nauczycielski, biblioteka szkolna, pokój pedagoga szkolnego, w których mogą przebywać inni użytkownicy tylko w obecności osób upoważnionych do korzystania z tych pomieszczeń; to samo dotyczy uczniów, ich rodziców oraz interesantów; nikt z osób postronnych nie może przebywać w pomieszczeniach bez zgody uprawnionych osób.

W strefie II do danych osobowych mają dostęp wszystkie osoby upoważnione do ich przetwarzania, a osoby postronne (uczniowie, ich rodzice i praktykanci) tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych.

Zabezpieczenia sprzętu.

1. W celu zapewnienia większego bezpieczeństwa i ochrony danych powinno wykorzystać się system operacyjny Microsoft Windows, posiadający rozbudowane mechanizmy nadawania uprawnień i praw dostępu. Dla pełnego wykorzystania mechanizmów należy stosować system plików NTFS, który zapewnia wsparcie mechanizmu ochrony plików i katalogów oraz mechanizmów odzyskiwania na wypadek uszkodzenia dysku lub awarii komputerów.
2. Administrator systemu informatycznego jest jedyną osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustalonych i statutowych zadań szkoły i posiadających ważną licencję użytkownika.
3. Bieżąca konserwacja sprzętu wykorzystywanego w szkole do przetwarzania danych prowadzona jest przez jej pracowników, przede wszystkim przez administratora systemu informatycznego.
4. Poważne naprawy wykonywane przez pracowników firm zewnętrznych realizowane są w budynku szkoły po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszanie bezpieczeństwa danych.
5. Dopuszcza się konserwowanie i naprawę sprzętu poza szkołą jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych, można zbyć dopiero po usunięciu danych osobowych, a urządzenia uszkodzone mogą być przekazywane do utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony szkoły) właściwym podmiotom, z którymi także zawiera się umowy powierzania przetwarzanych danych.
6. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, które podpisują osoby uczestniczące w naprawie lub konserwacji.

Zabezpieczenia we własnym zakresie.

W celu podniesienia bezpieczeństwa danych każda osoba upoważniona do przetwarzania danych lub użytkownik systemu informatycznego zobowiązani są do:

- 1) ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
- 2) niepozostawienia bez kontroli dokumentów i nośników danych w klasach i innych miejscach publicznych oraz w samochodach;
- 3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratki wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
- 4) niepodłączania do listew, podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
- 5) pilnego strzeżenia akt i nośników komputerowych;
- 6) kasowania po wykorzystaniu danych na dyskach przenośnych;
- 7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;
- 8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
- 9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
- 10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;
- 11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
- 12) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;
- 13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
- 14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
- 15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
- 16) kończenia pracy stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;
- 17) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy;

- 18) niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
- 19) zachowania tajemnicy danych, w tym także wobec najbliższych;
- 20) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
- 21) umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
- 22) zamykanie okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
- 23) zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
- 24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożeniu klucza sekretariacie szkoły. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów, zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym dyrektora szkoły, który zgłasza osobie sprzątającej jednorazową rezygnację z wykonywania swej pracy. W takim przypadku także należy zostawić klucz w kancelarii szkoły.

5. Wykorzystywanie akt i dokumentów szkolnych do pracy w domu.

1. Wykorzystywanie akt i dokumentów, zawierających dane osobowe do pracy w domu jest możliwe tylko po uzyskaniu upoważnienia na piśmie, udzielanego przez dyrektora szkoły lub jego zastępcę.
2. Administrator bezpieczeństwa informatycznego lub upoważniona przez niego osoba prowadzi ewidencję akt spraw i dokumentów szkolnych, wynoszonych przez uprawnionych pracowników.
3. Z wynoszonych dokumentów może korzystać wyłącznie upoważniony pracownik, który powinien dołożyć wszelkich starań, aby osoby postronne, w tym domownicy, nie mogły mieć do nich dostępu.
5. Upoważniony pracownik po zakończeniu wykonywania pracy w domu powinien niezwłocznie zwrócić dokumenty dyrektorowi szkoły lub jego zastępcy.
6. Pracownicy, wynoszący dokumenty i akta spraw do domu, są obowiązani do ochrony danych w nich zawartych i w razie ich udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym podlegają grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 zgodnie z art. 51 ustawy.

6. Postępowanie z nośnikami danych i ich bezpieczeństwo.

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

- 1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone.

- 2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;
- 3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;
- 4) po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wnosić poza siedzibę administratora danych.

Wymiana danych i ich bezpieczeństwo.

1. Sporządzanie kopii zapasowych następuje w trybie opisanym w pkt. 9. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
2. Pocztą elektroniczną można przysyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami” na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w internecie.
3. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora bezpieczeństwa informacji. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa informacji oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
4. Administrator systemu informatycznego w uzgodnieniu z ABI dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
5. Należy stosować następujące sposoby kryptograficznej ochrony danych:
 - przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP – tunelowanie, szyfrowanie połączenia,
 - przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron <https://>.

Komputery przenośne i praca na odległość.

W szkole używa się komputerów przenośnych, do przetwarzania danych osobowych, które uruchamia się po wprowadzeniu hasła.

Przeglądy okresowe, zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy).

1. Administrator bezpieczeństwa informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza osoby przetwarzające dane osobowe, są obowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.
2. Administrator bezpieczeństwa informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.
3. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora bezpieczeństwa informacji i administratora danych, w której usunięto dane osobowe.

Udostępnianie danych osobowych.

1. Udostępnianie danych osobowych policji i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem .
2. Udostępnianie informacji policji odbywa się według następującej procedury:
 - 1) udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
 - oznaczenie wnioskodawcy,
 - wskazanie przepisów uprawniających do dostępu do informacji,
 - określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
 - wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
 - 2) udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
 - 3) osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.

4) jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

5) jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępniania informacji.

6) Innym podmiotom dane osobowe, dotyczące pracowników i uczniów szkoły, nie mogą być udostępniane.

Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

Niezależnie od rozwiązania stosunku pracy osoby, popełniające przestępstwo, będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51 i 52. ustawy oraz art. 266. Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

- 1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
- 2) niezabezpieczenia nośnika lub komputera przenośnego,
- 3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

Przeglądy polityki bezpieczeństwa i audyty systemu.

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

- 1) zmian w budowie systemu informatycznego,
- 2) zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
- 3) zmian w obowiązującym prawie.

Administrator bezpieczeństwa informacji po uzgodnieniu z dyrektorem szkoły może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu

dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji, jak i dyrektora.

Dyrektor szkoły, biorąc pod uwagę wnioski administratora bezpieczeństwa informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

POSTANOWIENIA KOŃCOWE.

1. Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązana jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. Niezastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur ochrony danych jest traktowane jako ciężkie naruszenie obowiązków służbowych, skutkujące poważnymi konsekwencjami prawnymi włącznie z rozwiązaniem stosunku pracy na podstawie art. 52. Kodeksu pracy.
3. Polityka bezpieczeństwa, wchodzi w życie z dniem 15.05.2018r.