Załącznik Nr 1
do Zarządzenia Nr 7/2012
Dyrektora Zespołu Szkół Ogólnokształcących
w Sejnach

POLITYKA BEZPIECZEŃSTWA

ZESPOŁU SZKÓŁ OGÓLNOKSZTAŁĄCYCH W SEJNACH

1.1 INFORMACJE OGÓLNE

Niniejszy dokument Polityki Bezpieczeństwa został opracowany przez Administratora Danych Zespołu Szkół Ogólnokształcących w Sejnach, w celu zapewnienia zgodności przetwarzania danych osobowych z polskim ustawodawstwem.

Polityka Bezpieczeństwa wraz z instrukcją zarządzania systemami informatycznymi stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt. 1 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 z późn. zm.).

Polityka Bezpieczeństwa została wdrożona zarządzeniem dyrektora i obowiązuje od dnia 13 kwietnia 2012 r. Wszelkie wątpliwości dotyczące sposobu interpretowania zapisów niniejszego dokumentu Polityki Bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba mająca dostęp do danych osobowych z upoważnienia Administratora Danych, została zapoznana z Polityką Bezpieczeństwa i zobowiązana do jej przestrzegania w zakresie wynikającym z przedzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Osoby o których mowa, złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa oraz zobowiązały się do stosowania zawartych w niej postanowień.

1.2 CEL PRZYGOTOWANIA POLITYKI BEZPIECZEŃSTWA

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Polityki Bezpieczeństwa było zapewnienie zgodności działania Zespołu Szkół Ogólnokształcących w Sejnach z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Opracowany dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

1) *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 z późn. zm.),*
2) *ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),*
3) *ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256 poz. 2572 z późn. zm.),*
4) *rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2002 r. Nr 23, poz. 225 z późn. zm.),*
5) *ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (tj. Dz. U. z 2001 r. nr 128, poz. 1402 z późn. zm.).*

Zadaniem Polityki Bezpieczeństwa jest określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

1.3 ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES STOSOWANIA

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Zespołu Szkół Ogólnokształcących w Sejnach. Na Politykę Bezpieczeństwa składają się następujące informacje:

1) *wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,*
2) *wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,*
3) *opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi,*
4) *sposób przepływu danych pomiędzy poszczególnymi systemami,*
5) *określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.*

Politykę Bezpieczeństwa stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Polityki Bezpieczeństwa.

1.4 SPOSÓB AKTUALIZACJI POLITYKI BEZPIECZEŃSTWA

Administrator Danych zobowiązuje się dokonywać corocznie przeglądu i aktualizacji Polityki Bezpieczeństwa. Weryfikacja zapisów Polityki Bezpieczeństwa jest prowadzona pod kątem zgodności stanu deklarowanego ze stanem faktycznym. Do końca stycznia każdego roku kalendarzowego Administrator Danych lub osoba przez niego upoważniona dokona sprawdzenia aktualności Polityki Bezpieczeństwa.
Polityka bezpieczeństwa podlega aktualizacji każdorazowo w przypadku likwidacji, utworzenia lub zmiany zawartości zbioru danych, a także w przypadku zmiany przepisów prawa dotyczących ochrony danych osobowych, wymagającej aktualizacji Polityki.
Aktualizacja Polityki Bezpieczeństwa jest przeprowadzona przez Administratora Danych. Nowa wersja Polityki Bezpieczeństwa zastępuje poprzednio obowiązującą.

1.5 SPOSÓB PRZECHOWYWANIA DOKUMENTU POLITYKI BEZPIECZEŃSTWA

Dokument Polityki Bezpieczeństwa jest przechowywany w wersji elektronicznej, na komputerze zabezpieczonych przez dostępem osób nieupoważnionych. Zapewniona jest możliwość wydrukowania aktualnej wersji dokumentu Polityki Bezpieczeństwa w terminie 12 godzin od pojawienia się takiej potrzeby.
Dokument Polityki Bezpieczeństwa jest przechowywany wraz z innymi dokumentami, do których dostęp posiada tylko Administrator Danych oraz upoważnione przez niego osoby. Wydrukowany po aktualizacji dokument Polityki Bezpieczeństwa zastępuje poprzedni, który ulega zniszczenia.

1.6 WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1) *ustawa – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997 r. Nr 133 poz. 883 z późn. zm.), zwaną dalej „ustawę",*
2) *rozporządzenie – 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 z późn. zm.), zwane dalej „rozporządzeniem",*
3) *dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,*
4) *polityka bezpieczeństwa – dokument polityki bezpieczeństwa w rozumieniu § 1 pkt. 1 rozporządzenia, zwaną dalej „polityką",*
5) *instrukcja zarządzania systemem informatycznym – dokument instrukcji zarządzania systemem informatycznym w rozumieniu § 1 pkt. 1 rozporządzenia, zwaną dalej „instrukcją",*
6) *zbiór danych – 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,*
7) *przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takiej jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,*
8) *system informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,*
9) *zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę przez ich nieuprawnionym przetwarzaniem,*
10) *usuwaniu danych – rozumie się przez te zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,*
11) *administrator danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych,*
12) *zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie,*
13) *odbiorca danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:*
    - *osoby, której dane dotyczą,*
    - *osoby upoważnionej do przetwarzania danych,*
    - *przedstawiciela, o którym mowa w art. 31 a ustawy o ochronie danych osobowych,*
    - *podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,*
    - *organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,*
14) *identyfikator użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,*
15) *hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,*
16) *sieć telekomunikacyjna – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852 , z późn. zm.),*

17) *sieć publiczna – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne,*
18) *teletransmisja – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,*
19) *rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,*
20) *integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,*
21) *raport – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,*
22) *poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,*
23) *uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.*

2. WYKAZ ZBIORÓW DANYCH WRAZ ZE WSKAZANIEM PROGRAMÓW WSKAZANYCH DO PRZETWARZANIA TYCH DANYCH

Dane osobowe gromadzone są w zbiorach:

Zbiór 1 – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;
Zbiór 2 – Akta osobowe pracowników
Zbiór 3 – Dokumentacja dotycząca polityki kadrowej – awanse, nagrody itp.
Zbiór 4 – Ewidencja zwolnień lekarskich
Zbiór 5 – Skierowania na badania okresowe
Zbiór 6 – Ewidencja SIO
Zbiór 7 - Dokumentacja funduszu socjalnego
Zbiór 8 – Listy płac pracowników
Zbiór 9 – Kartoteki zarobkowe pracowników
Zbiór 10 – Deklaracje ubezpieczeniowe pracowników
Zbiór 11 – Deklaracje i kartoteki ZUS pracowników
Zbiór 12 – Deklaracje podatkowe pracowników
Zbiór 13 – Księga uczniów
Zbiór 14 – Arkusze ocen
Zbiór 15 – Podanie uczniów o przyjęcie do szkoły
Zbiór 16 – Dzienniki zajęć obowiązkowych i dodatkowych
Zbiór 17 – Rejestr zaświadczeń wydanych pracownikom szkoły
Zbiór 18 – Rejestr wypadków uczniów
Zbiór 19– Teczki awansu zawodowego
Zbiór 20– Arkusz organizacji placówki

Nr	*Nazwa zbioru danych*	*Systemy informatyczne stosowane do przetwarzania danych osobowych w zbiorze*	*Zastosowany poziom bezpieczeństwa*
1	*uczniowie oraz kandydaci do szkoły*	*Word, Excel, OKE, Vulcan Optivum Świadectwa*	*wysoki*
2	*pracownicy oraz kandydaci do pracy*	*Word, Excel,*	*wysoki*
3	*rodzice / prawni opiekunowie*	*Word, Excel*	*wysoki*
4	*płace*	*Vulcan Optivum Płace, HomeNet, Płatnik - ZUS*	*wysoki*

3. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY POSZCZEGÓLNYMI POLAMI INFORMACYJNYMI

L.p.	Nazwa zbioru	Zakres przetwarzania danych
1	uczniowie oraz kandydaci do szkoły	imię, nazwisko, data urodzenia, nr PESEL, adres zamieszkania, klasa, data przyjęcia do szkoły, oceny, obecność na zajęciach, dokumentacja medyczna, oceny z zachowania
2	pracownicy oraz kandydaci do pracy	imię (imiona) i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), numer telefonu, wykształcenie, przebieg dotychczasowego zatrudnienia, numer PESEL i NIP, imiona i nazwiska oraz daty urodzenia dzieci pracownika
3	rodzice / prawni opiekunowie	imiona i nazwiska, adres zamieszkania, numer telefonu
4	płace	wysokość wynagrodzenia pracowników, imię /imiona) i nazwisko, data i miejsce urodzenia, miejsce zamieszkania i zameldowania,numer telefonu, numery kont bankowych, numer NIP i PESEL

4. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

Nr	Źródłowy system informatyczny	Docelowy system informatyczny	Zakres przesyłanych danych osobowych	Sposób transmisji
1	Word / Excel	Word/Excel	imię i nazwisko ucznia, data i miejsce urodzenia, PESEL adres zamieszkania /zameldowania	manualny /eksport oraz import/
2		SIO	PESEL pracowników, dane o wynagrodzeniu, zatrudnieniu, wykształceniu	przesyłanie danych poprzez sieć telekomunikacyjną
3		OKE	imię i nazwisko ucznia, data i miejsce urodzenia, PESEL	przesyłanie danych przez sieć telekomunikacyjną
4		HomeNet	imię i nazwisko pracownika, numer konta, wysokość przelewu	przesyłanie danych przez sieć telekomunikacyjną
5		Płatnik-ZUS	imię i nazwisko pracownika, data urodzenia, PESEL, adres zamieszkania i zameldowania, numer telefonu	przesyłanie danych poprzez sieć telekomunikacyjną
6		eRU-PZU	imię i nazwisko pracownika, data urodzenia, PESEL, adres zamieszkania	przesyłanie danych przez sieć telekomunikacyjną

5. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Dane osobowe gromadzone i przetwarzane są w budynku szkolnym, mieszczącym się w Sejnach przy ul. Łąkowej 1.

Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są:

1) *sekretariat szkoły – I piętro*
2) *gabinet dyrektora – I piętro*
3) *gabinet wicedyrektora – I piętro*
4) *gabinet księgowych – I piętro*
5) *biblioteka szkolna – I piętro*
6) *gabinet psychologa – I piętro*
7) *pokój nauczycielski - parter*
8) *archiwum szkolne – parter*

6. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

Rodzaje zagrożeń naruszających ochronę danych osobowych:

1. Zagrożenia losowe:

1) *zewnętrzne np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona, jednak nie dochodzi do naruszenia danych osobowych;*
2) *wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenia ciągłości pracy systemu i naruszenia poufności danych.*

2. Zagrożenia zamierzone (świadome i celowe naruszenie poufności danych) – wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:

1) *nieuprawniony dostęp do systemu z zewnątrz;*
2) *nieuprawniony dostęp do systemu z wewnątrz;*
3) *nieuprawnione przekazanie danych;*
4) *bezpośrednie zagrożenie*
5) *materialnych składników np. kradzież, zniszczenie.*

3. Okoliczności zakwalifikowane, jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenie systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

1) *sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonym prac remontowych;*
2) *niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;*
3) *awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;*
4) *naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie*
5) *modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;*

6) *ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania;*
7) *podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;*
8) *rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych itp.);*
9) *nieprawidłowości w zakresie zabezpieczenie miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum)).*

4. Szczegółowe zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych reguluje Instrukcja Zarządzania Systemami Informatycznymi służącym do przetwarzania danych osobowych.

7. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Formy zabezpieczeń pomieszczeń, w których przechowywane są dane osobowe:
1) *wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenie przez ostatnią osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;*
2) *dane osobowe przechowywane w wersji tradycyjnej (papierowej) i elektronicznej (płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w sejfach;*
3) *nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;*
4) *budynek, w którym przetwarzane są dane jest całodobo monitorowany.*

2. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:
1) *udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez administratora sieci następuje na podstawie upoważnienia do przetwarzania danych osobowych;*
2) *identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania;*
3) *udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym;*
4) *ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe;*

3. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
1) *odrębne zasilanie sprzętu komputerowego lub zastosowanie zasilaczy zapasowych UPS;*
2) *ochrona przed utratą danych poprzez cykliczne wykonywanie kopii zapasowych;*
3) *zapewnienie właściwej temperatury i wilgotności w pomieszczeniach;*
4) *zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w dostępnej odległości gaśnic.*

4. Organizację ochrony danych osobowych realizuje się poprzez:
1) *zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;*
2) *przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów;*
3) *kontrolowanie pomieszczeń budynku;*
4) *prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;*
5) *wyznaczenie administratora bezpieczeństwa informacji.*

DYREKTOR
Zespołu Szkół Ogólnokształcących
w Sejnach
mgr inż. Andrzej Małkiński