Załącznik nr 1 do zarządzenia nr 11/2012
Dyrektora SP nr 2 w Żarach
z dn. 30 sierpnia 2012r.

POLITYKA BEZPIECZEŃSTWA

w zakresie sposobu przetwarzania danych osobowych oraz środków ich ochrony w Szkole Podstawowej nr 2 w Żarach

§ 1
Podstawa prawna

1. Art. 36 *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (tekst jedn.: DzU 2002 nr 101, poz. 926 ze zm.).
2. § 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* (DzU 2004 nr 100, poz. 1024).

§ 2
Postanowienia ogólne

"*Polityka bezpieczeństwa w zakresie sposobu przetwarzania danych osobowych oraz środków ich ochrony w Szkole Podstawowej nr 2 w Żarach"* jest dokumentem zwanym dalej ***"Polityką bezpieczeństwa"***, który określa zbiór zasady, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony oraz dystrybucji przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym ujawnieniem. Dokument opisuje wewnętrzną strukturę odpowiedzialności za przetwarzane przez Szkołę dane osobowe.

Celem "Polityki bezpieczeństwa" jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych. ***„Polityka bezpieczeństwa" zawiera w szczególności:***

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- sposób przepływu danych pomiędzy poszczególnymi systemami,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i obliczalności przy przetwarzaniu danych osobowych.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w Szkole Podstawowej nr 2, jak i innych, np. studentów, odbywających w nim praktyki pedagogiczne.

„Dane osobowe" są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Możliwa do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny (np. PESEL, NIP) albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

W celu zapewnienia bezpieczeństwa przetwarzanych danych wymaga się, aby wszyscy jego użytkownicy byli świadomi konieczności ochrony wykorzystywanych zasobów. Odpowiedzialność za powierzone dane osobowe, ponoszą wszyscy pracownicy szkoły, mający dostęp do danych osobowych w ramach swych obowiązków służbowych. Świadomość tejże odpowiedzialności potwierdzają własnoręcznym podpisem.

Pracownicy są odpowiedzialni za bezpieczeństwo danych, do których mają dostęp. W szczególności w systemach informatycznych odpowiadają oni za poprawne wprowadzanie informacji do tych systemów oraz za użycie, zniszczenie lub uszkodzenie sprzętu oraz znajdujących się na nim danych i oprogramowania. Konsekwencją nie stosowania przez pracownika środków bezpieczeństwa określonych w instrukcjach wewnętrznych może być zniszczenie części lub całości systemów informatycznych, utrata poufności, autentyczności, straty finansowe, jak również utrata wizerunku

§ 3

Pojęcia

Ilekroć w dokumencie jest mowa o:

1. **Ustawie**– rozumie się przez to *ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997 r.* (tekst jedn.: DzU 2002 nr 101, poz. 926 ze zm.);

2. **Administratorze danych osobowych** – rozumie się przez to Dyrektora Szkoły Podstawowej nr 2 w Żarach;

3. **Administratorze bezpieczeństwa informacji (ABI)** – rozumie się przez to osobę powołaną przez administratora danych, która odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym szkoły oraz tradycyjnym systemie, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w

których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;

4. **Osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to każdego pracownika szkoły upoważnionego przez administratora danych do przetwarzania danych osobowych;

5. **Danych osobowych**– w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące osoby fizycznej, zidentyfikowanej lub możliwej do zidentyfikowania;

6. **Przetwarzaniu danych osobowych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

7. **Zbiorze 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;

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

9. **Użytkowniku** - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

10. **Identyfikatorze użytkownika (login)** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

11. **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

12. **Uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

13. **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

14. **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

15. **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;

16. **Serwisancie -** rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;

17. **Szkole -** rozumie się przez to Szkołę Podstawową nr 2 w Żarach.

§ 4

Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych, reprezentowany przez dyrektora szkoły, realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

   a) 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,

   b) 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,

   c) wyznacza administratora bezpieczeństwa informacji oraz administratora sieci oraz określa zakres ich zadań i czynności,

   d) 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,

   e) zapewnia we współpracy z administratorem bezpieczeństwa informacji i systemu użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,

   f)) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur.

2. Administrator bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem ochrony danych osobowych, w tym zwłaszcza:

   a) sprawuje nadzór nad wdrożeniem stosowanych środków fizycznych, a także organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych,

   b) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,

   c) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych,

   d) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,

   e) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz w razie potrzeby prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych,

   f) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych,

g) prowadzi oraz aktualizuje dokumentację, opisującą sposób przetwarzanych danych osobowych oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych,

h) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,

i) przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków osób upoważnionych do przetwarzania danych osobowych,

j) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych,

k) w porozumieniu z administratorem danych osobowych na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

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

a) 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,

b) 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,

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

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

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

f) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

§ 5

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.
2. Określając obszar przetwarzania danych osobowych w Szkole wzięto pod uwagę zarówno miejsca, w których wykonuje się operacje na danych osobowych, jak również miejsca, gdzie przechowuje się wszelkie nośniki zawierające dane osobowe. Dane przetwarzane są w budynkach szkolnych znajdujących się w Żarach przy ulicy: W. Witosa 25, G. Zapolskiej 12 oraz dwóch salach gimnastycznych przy wyżej wymienionych budynkach. Ze względu na szczególne nagromadzenie danych osobowych szczególnie chronione powinny być następujące pomieszczenia :

   a) gabinet dyrektora szkoły, b) gabinet wicedyrektora, c) sekretariat, d) pokoje nauczycielskie, e) pokój pedagoga, logopedy, pielęgniarki i psychologa, f) biuro głównej księgowej, g) sale lekcyjne, h) archiwum szkolne, a także i) szafa aktowa, szafy w sekretariacie, szafki w pokojach nauczycielskich na dzienniki, sejf, komputery, serwery firm zewnętrznych (Librus, ZUS, MEN, OKE, strona internetowa szkoły), komputerowe, także zewnętrzne nośniki danych.

3. W szczególnie uzasadnionych przypadkach dane osobowe mogą być przetwarzane poza siedzibą administratora danych, czyli poza Szkołą. Dotyczy to danych osobowych zawartych w klasówkach, sprawdzianach, kartkówkach oraz protokolarzu rad pedagogicznych. Osobę upoważnioną do przetwarzania danych osobowych, która wynosi wymienioną powyżej dokumentację poza siedzibę Szkoły, obowiązuje zakaz udostępniania tejże dokumentacji osobom trzecim, np. członkom rodziny. Osoba wynosząca w/w dokumentację w celu jej sprawdzenia lub napisania protokołu z posiedzenia rady pedagogicznej, szczególnie rady klasyfikacyjnej i podsumowującej, musi ten fakt zgłosić administratorowi danych (dyrektorowi) i uzyskać jego zgodę.

§ 6

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

lp.	Nazwa zbioru danych osobowych	Nazwy programów komputerowych do przetwarzania zbiorów danych	Nazwy zasobów, w których gromadzone są dane dotyczące zbioru danych osobowych	Lokalizacja miejsca, w którym znajdują się zbiory danych osobowych
1	Uczniowie (kandydaci na uczniów) oraz ich rodzice (prawni opiekunowie)	SIO (stare i nowe), Program e-dziennik, Program do drukowania świadectw: Librus, Vulcan, Program	Księga ewidencji, księga uczniów, wykaz dzieci zamieszkałych w obwodzie szkoły, dzienniki lekcyjne, arkusze ocen, dokumentacja medyczna,	Sekretariat, gabinet pielęgniarki, dyrektora , wicedyrektora, pokój nauczycielski, pedagoga, psychologa, logopedy, szafa w

		Vulkan – Sekretariat Uczniów Optivum, Microsoft Office, Word i Execel, OKE, Moll, PEFRON.	dokumentacja psychologiczno-pedagogiczna. Lista kandydatów na uczniów, program obsługujący system CCTV.	sekretariacie, serwery zew., komputer dyrektora, wicedyrektora i kierownika, gospodarczego. Strona internetowa szkoły.
2	Dane kadrowe i płacowe (byli i obecni pracownicy)	SIO (stare i nowe), Programy kadrowo – płacowe: Vulcan – Księgowość Optivum, Płace Optivum, Program SJO Bestia, Program Płatnik, Program Podpisów Elektronicznych, Program Vulkan – Kadry oraz Arkusz Optivum, Program e-dziennik, serwery Banku Zachodniego, GUS.	Akta osobowe, dokumentacja dyrektora, wicedyrektora, kierownika gospodarczego, księgowego, dokumentacja archiwalna, program obsługujący system CCTV.	Sekretariat, gabinet księgowego, dyrektora , wicedyrektora, szafa w sekretariacie, segregatory w gabinecie dyrektora, serwery zew., komputer dyrektora, wicedyrektora , księgowego, kierownika gospodarczego, nośniki komputerowe, archiwum, strona internetowa szkoły.
3	Potencjalni pracownicy	Brak – do przetwarzania danych w tym zbiorze nie są wykorzystywane żadne systemy informatyczne.	Teczka z podaniami osób starających się o przyjęcie do pracy.	Sekretariat, gabinet dyrektora, szafa w sekretariacie.
4	Rejestr korespondencji	Brak – do przetwarzania danych w tym zbiorze nie są wykorzystywane żadne systemy informatyczne.	Rejestr korespondencji.	Sekretariat, szafa w sekretariacie.
5	Nagrania monitoringu	Brak – do przetwarzania danych w tym zbiorze nie są wykorzystywane żadne systemy informatyczne.	Urządzenie nagrywające telewizji przemysłowej (macierz dyskowa).	Pokój nauczycielski.
6	Kontrahenci	Programy Vulcan: Księgowość Optivum, Magazyn Optiwum, Płatnik, Microsoft Office, Word i Execel.	Dokumentacja zamówień publicznych, dokumentacja intendenta, dokumentacja księgowego.	Sekretariat, gabinet dyrektora, księgowego, komputer dyrektora, księgowego, kierownika gospodarczego, intendenta.

7	Uczniowie realizujący obowiązek szkolny w innych placówkach	SIO (stare i nowe).	Księga ewidencji, wykaz dzieci zamieszkałych w obwodzie szkoły.	Sekretariat, gabinet dyrektora, szafa w sekretariacie, komputer kierownika gospodarczego.

1. Do każdego ze zbiorów danych, które są przetwarzane za pomocą systemu informacyjnego stosuje się wysoki poziom bezpieczeństwa.

§ 7
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

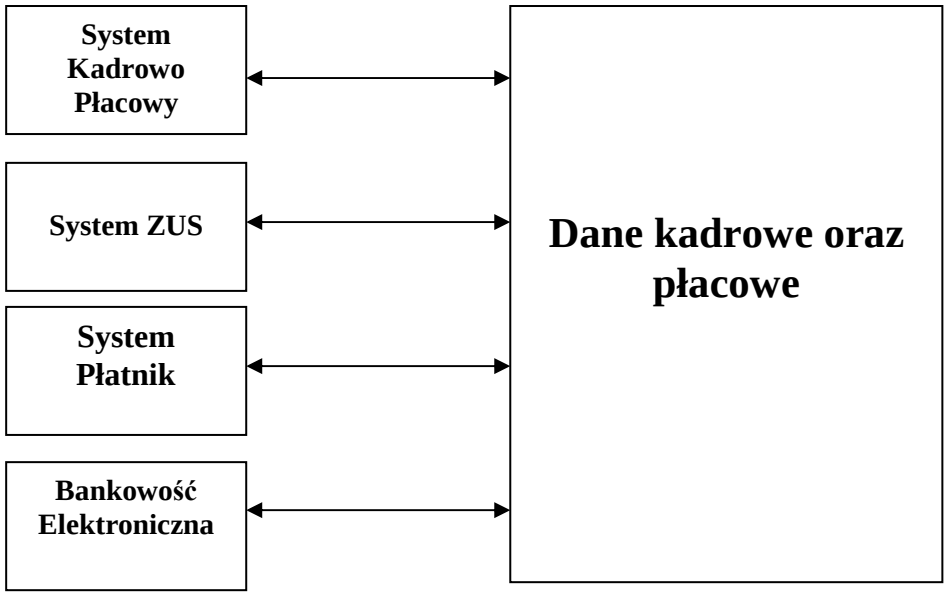
1. Poniższa tabela przedstawia opis struktury zbiorów danych oraz zakres informacji gromadzonych w danym zbiorze:

lp.	Nazwa zbioru	Opis struktury zbioru danych, zakres przetwarzanych danych
1	Uczniowie (kandydaci na uczniów) oraz ich rodzice (prawni opiekunowie)	Imię (imiona), nazwisko, imiona i nazwiska rodziców (prawnych opiekunów), data i miejsce urodzenia, miejsce zameldowania i zamieszkania, miejsce zamieszkania rodziców (prawnych opiekunów), miejsce realizowania obowiązku rocznego przygotowania do szkoły, data przyjęcia do szkoły, klasa, data ukończenia szkoły, numer PESEL, dane o stanie zdrowia, nr telefonu rodziców (prawnych opiekunów), wizerunek, oceny, wyniki badań psychologiczno-pedagogicznych, formy pomocy, dochód na jedną osobę w rodzinie, dane osób pozostających we wspólnym gospodarstwie domowym - imię i nazwisko, data urodzenia, stopień pokrewieństwa, przesłanki wskazujące na trudną sytuację w rodzinie.
2	Dane kadrowe i płacowe (byli i obecni pracownicy)	Imię (imiona), nazwisko, imiona rodziców, data i miejsce urodzenia, miejsce zamieszkania, wykształcenie, stopień awansu zawodowego, przebieg dotychczasowego zatrudnienia, informacja o niekaralności, dodatkowe uprawnienia, zainteresowania, numer i seria dowodu osobistego, organ wydający dowód osobisty, PESEL, NIP, dane dotyczące stanu zdrowia, wizerunek adres e-mail, nr telefonu, data zatrudnienia, płeć, numer konta bankowego, wysokość dochodów na członka rodziny, stan rodzinny cywilny i rodzinny (imię i nazwisko dziecka, data urodzenia), osoba, którą powiadomić w razie wypadku.
3	Potencjalni pracownicy	Imię (imiona), nazwisko, imiona rodziców, data i miejsce urodzenia, miejsce zamieszkania, wykształcenie, stopień awansu zawodowego, przebieg dotychczasowego zatrudnienia, płeć, wizerunek, adres e-mail, numer telefonu.
4	Rejestr korespondencji	Imię i nazwisko, adres nadawcy, data wpłynięcia , temat korespondencji.
5	Nagrania monitoringu	Data, godzina, wizerunek.
6	Kontrahenci	Imię, nazwisko, nazwa i adres firmy, telefon, NIP, REGON, rodzaj usługi, zamówienia, należności, data sprzedaży, data zamówienia.

7	Uczniowie realizujący obowiązek szkolny w innych placówkach	Imię, nazwisko, adres zameldowania, data urodzenia, miejsce urodzenia, imiona I nazwiska rodziców, PESEL, placówka, w której realizowany jest obowiązek szkolny.

§ 8
Sposób przepływu danych pomiędzy systemami

1. W szkole pomiędzy poszczególnymi systemami nie dochodzi do przepływu danych. Dane ze zbiorów danych „Uczniowie" i „Pracownicy" są do systemu wprowadzane manualnie przez użytkownika, który wprowadza dane do systemów: SIO, OKE, E-dziennik. Do Systemów Sekretariat Uczniów, Kadry, Arkusz Organizacyjny, E-dziennik dane są wprowadzane manualnie przez użytkownika.
2. Przepływ danych zachodzi między systemami Księgowość, Kadrowo-Płacowym, Płatnik, ZUS, Bankowość Elektroniczna:



§ 9

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i obliczalności przy przetwarzaniu danych osobowych

1. Szkoła przetwarza dane osobowe na podstawie przepisów prawa. Dane osobowe mogą być udostępniane zgodnie z art. 29 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. W celu zapewnienia p i rozliczalności przetwarzanych danych osobowych stosuje się poniższe środki ochrony fizycznej, środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej oraz odpowiednie środki organizacyjne:
    a) budynki szkoły objęte są systemem kontroli dostępu, w tym sygnalizacji włamania;

b) elektroniczne systemy monitoringu pozwalają na kontrole ruchu osób i informują Firmę Ochrony Mienia o przypadkach nieautoryzowanego wejścia;

c) w szkole dokonuje się przeglądu gaśnic i stosuje się przepisy przeciwpożarowe;

d) dzienniki są przechowywane w zamkniętych szafkach w pokojach nauczycielskich; nie wolno udostępniać ich uczniom lub postronnym osobom bez nadzoru; inna dokumentacja papierowa oraz kopie zapasowe także w zamkniętych szafkach w pomieszczeniach, w których przetwarza się dane osobowe, pieczątki i kopie zapasowe księgowości oraz inne ważne dokumenty, np. czeki bankowe sa przechowywane w sejfie;

e) w obszarze przetwarzania danych osoby postronne mogą przebywać za zgodą administratora danych lub w towarzystwie osób upoważnionych do przetwarzania danych;

f) każdy pracownik szkoły przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się oraz stosowania przepisów ustawy ochronie danych osobowych i instrukcji wewnątrzszkolnych, co potwierdza podpisem;

g) pomieszczenia, w których przetwarzane są dane zamykane są na klucz, jeżeli nie przebywa w nim osoba uprawniona; klucze od sal lekcyjnych są zamykane w pokojach nauczycielskich, gabinetów dyrektora i wicedyrektora, księgowej i sekretariatu posiadają osoby sprzątające i kierownik gospodarczy, klucze od szkoły posiadają woźni oraz kierownik gospodarczy; nie wolno zostawiać kluczy w zamkach,

h) w szkole funkcjonuje monitoring, monitory ustawione są w sposób uniemożliwiający oglądanie ekranu z miejsc ogólnodostępnych, są w pokoju nauczycielskim,

i) bieżące naprawy komputera, dokonywane są w obecności użytkownika systemu lub po pozbawieniu tych urządzeń zapisów;

j) administrator bezpieczeństwa informatycznego jest osobą uprawnioną do nadzoru 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 użytkowania;

k) wykorzystywanie akt i dokumentów, zawierających dane osobowe (dzienniki zajęć), do pracy w domu jest kategorycznie zabronione; wyjątkiem są kartkówki, sprawdziany i księga protokołów rady pedagogicznej;

l) dane z nośników przenośnych nie będących 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 służbowych, nie prywatnych; nośniki te muszą być przechowywane w zamkniętych na klucz szafach, biurkach i nie udostępniane osobom postronnym; po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

m) 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 wynosić poza siedzibę administratora;

n) pracownicy, po zakończonej pracy są zobowiązani do stosowania zasady „czystego biurka”;

o) pocztą elektroniczną można przesyłać 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, nie należy korzystać z formy „prześlij do wszystkich”;

p) przed atakami z sieci zewnętrznej wszystkie komputery administratora danych 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.

q) w szkole stosowane są programy antywirusowe: Avast, Antivirus 5, Kasperski oraz urządzenia UPS, które chronią przed utratą danych w razie awarii zasilania prądu; wykonuje się także kopie zapasowe ważnych dokumentów, głównie kadrowo-płacowych, arkusza organizacyjnego, danych sekretariatu;

r) monitory komputerów, na których przetwarzane są dane osobowe należy ustawiać tak, by uniemożliwić w nie wgląd osobom postronnym;

s) administrator bezpieczeństwa informacji 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;

t) osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania; administrator bezpieczeństwa przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem, hasła należy zmieniać co 30 dni, powinny zawierać 8 znaków, małe i duże litery i cyfry;

u) do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji i pracowników działu informatyki;

v) operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać główny księgowy; upoważniony przez dyrektora, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek, należy złożyć dwa podpisy elektroniczne;

w) w szkole nie używa się komputerów przenośnych do przetwarzania danych osobowych, z wyjątkiem laptopa administratora danych, dyrektora szkoły; odpowiedzialnym za monitorowanie dostępu do systemu i jego użycia jest administrator bezpieczeństwa informacji;

x) administrator bezpieczeństwa informacji przeprowadza co najmniej 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;

y) z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora bezpieczeństwa informacji i administratora danych, w której usunięto dane osobowe;

z) udostępnianie danych osobowych policji, służbie miejskiej i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem, udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji, wniosek ten powinien mieć formę pisemną;

aa) 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;

bb) w szkole prowadzi się szkolenia z zakresu ochrony danych osobowych oraz dokumentację opisującą sposoby przetwarzania danych.

§ 10
Przeglądy polityki bezpieczeństwa i audyty systemu

1. 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.
2. Administrator bezpieczeństwa informacji analizuje czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   a) zmian w budowie systemu informatycznego,
   b) zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych;
   c) zmian w obowiązującym prawie.
3. 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.

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

§ 11
Postanowienia końcowe

1. Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązania jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. 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 jest traktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące poważnymi konsekwencjami, włącznie z 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.
3. Polityka bezpieczeństwa, wchodzi w życie z dniem 1 września 2012 roku.

(miejscowość, data) (podpis i pieczęć dyrektora)