Załącznik do zarządzenia nr 4 KZ/ 2011

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE MUZYCZNEJ I STOPNIA W DOBCZYCACH

I. POSTANOWIENIA WSTĘPNE.

1. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, w Szkole Muzycznej I stopnia w Dobczycach, 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 Szkole Muzycznej I stopnia w Dobczycach jak i innych, np. studentów, odbywających w nim praktyki pedagogiczne.

II. DEFINICJE.

Definicje

Ilekroć w instrukcji jest mowa o:

administratorze danych – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych,

administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,

administratora systemu – rozumie się przez to dyrektora szkoły zatrudnionego w szkole.

haśle – 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 Szkołę Muzyczną I stopnia w Dobczycach.

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 (Dz. U. z 2002 r., nr 101, poz. 926. z późn. zm.)

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

użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH.

1. Administrator danych osobowych.

Administrator danych osobowych, reprezentowany przez dyrektora szkoły, 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 we współpracy z administratorem bezpieczeństwa informacji i systemu użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,

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

2. Administrator bezpieczeństwa informacji.

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

1) sprawuje nadzór nad wdrożeniem stosowanych środków fizycznych, a także organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych;
2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;

3) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych;

4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;

5) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych;

6) zawiera wzory dokumentów (odpowiednie klauzule w dokumentach), dotyczących ochrony danych osobowych;

7) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych;

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

9) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;

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

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

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

3. Administrator systemu.

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 katem ich dalszej przydatności do odtwarzania danych w przypadki 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.

W szkole funkcję administratora bezpieczeństwa informacji i administratora systemu ze względów organizacyjnych i finansowych (brak środków finansowych na zatrudnienie osoby, która realizowałaby obowiązki administratora bezpieczeństwa informacji) pełni jedna osoba. Rozdzielenie tych funkcji nastąpi po uzyskaniu od organu prowadzącego szkołę funduszy na zatrudnienie administratora bezpieczeństwa informacji.

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 Szkoły Muzycznej I stopnia w Dobczycach składa się z sieci wewnętrznej, mieszczącej się w pomieszczeniach szkoły i jest połączona siecią zbudowaną w oparciu o łącza dzierżawione w Neostradzie. Informacje przetwarzane w tej strukturze są jawne, ale podlegają ochronie zgodnie z przepisami ustawy.

2. W ramach tej struktury funkcjonuje oddzielnie system finansowy, za który odpowiada główny księgowy, oraz system zainstalowany w sekretariacie szkoły, które pracują oddzielnie.

3. Aplikacje (finansowo-księgowa – znajduje się przy Urzędzie Gminy i Miasta Dobczyce – odpowiedzialny kierownik ZOBJO, uczniowska – znajduje się w szkole) i wszystkie dane znajdują się na lokalnym twardym dysku pojedynczych komputerów. Modemy pozwalają na dostęp do internetu. Wymiana danych możliwa jest za pośrednictwem takich nośników, jak: dyskietki, płyty

CD-ROM, przenośnej pamięci USB, oraz za pośrednictwem usług internetowych – poczty elektronicznej. Jako system operacyjny wykorzystywany jest Windows XP Microsoft.

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

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. Dane osobowe przetwarzane są tylko i wyłącznie na terenie szkoły przy ul. Rynek 22a

3. Ze względu na szczególne nagromadzenie danych osobowych szczególnie chronione powinny być następujące pomieszczenia znajdujące się w budynku szkoły:

1) sekretariat szkoły;
2) gabinet dyrektora szkoły,

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

1. WYKAZ ZBIORÓW.

Lp.	Nazwa zbioru danych	Programy zastosowane do przetwarzania danych/nazwa zasobu danych	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1.	Kandydaci do szkoły	Open Office	sekretariat	parter-sekretariat
2.	Uczniowie szkoły	1. Księga uczniów	sekretariat	sekretariat
		2. Dzienniki lekcyjne	sekretariat	sekretariat
		3. Arkusze ocen	sekretariat	sekretariat
3.	Pracownicy szkoły	1. Akta osobowe	sekretariat	sekretariat
		2. SIO	sekretariat	sekretariat
		3. Arkusz organizacyjny	sekretariat	sekretariat
		4. Edytor tekstu	sekretariat, gabinet dyrektora	sekretariat, gabinet dyrektora

2. WYKAZ PROGRAMÓW STOSOWANYCH W SZKOLE:

- Windows XP,
- Office XP,
- NOD 32,
- SIO- System Informacji Oświatowej,

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

1. Zbiór danych „Kandydaci do szkoły".

Zbiór ten obejmuje dane osobowe kandydatów szkół, ubiegających się o przyjęcie do szkoły.

1) Zakres pierwszych danych tego zbioru, tzn. imię (imiona) i nazwisko kandydata, data i miejsce urodzenia, PESEL, adres zamieszkania, numer gimnazjum, do którego uczęszcza, imię i nazwisko rodziców (prawnych opiekunów) , ich adres zamieszkania , numer telefonu, dostępny jest członkom szkolnej komisji rekrutacyjno-kwalifikacyjnej, dyrektorowi szkoły i jego zastępcy oraz sekretarce, która wspiera komisję w pracach związanych z naborem kandydatów – przygotowaniem list przyjętych i ich uaktualnieniem oraz zbieraniem dokumentacji od kandydatów.

Dane osobowe kandydatów i ich rodziców znane są członkom komisji rekrutacyjno- kwalifikacyjnej i pozostałym osobom, uczestniczącym w procedurze naboru, w dniu ogłoszenia wyników naboru.

Wykazy kandydatów, przyjętych do szkoły, są upubliczniane wraz z ich danymi: imionami i nazwiskami oraz punktacją na tablicy informacyjnej w dniu ogłoszenia wyników.

Dane tego zakresu przetwarzane są za pomocą programu Open Office który wprowadził do użytku organ prowadzący szkołę. Jest on uruchamiany przez administratora bezpieczeństwa informacji za pomocą identyfikatora i hasła. Dostęp do niego ma sekretarka. Mogą być udostępniane zarówno organowi prowadzącemu szkołę (Urząd Gminy i Miasta Dobczyce), jak i organowi nadzorującemu szkołę, (CEA Warszawa) w celu opracowywania raportów o wynikach naboru kandydatów do szkoły muzycznej.

2) Zakresu drugi danych tego zbioru obejmuje wizerunek kandydatów przyjętych do szkoły i ich rodziców, którzy w dniu ogłoszenia wyników naboru i kilku następnych dniach, tj.: do dnia ostatecznego zamknięcia list przyjętych, pojawiają się w szkole.

2. Zbiór danych „Uczniowie szkoły".

Zbiór ten obejmuje dane osobowe uczniów i ich rodziców: imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, adres zamieszkania, PESEL oraz imiona i nazwisko rodziców (prawnych opiekunów), adres zamieszkania, numer telefonu domowego lub do pracy.

1) Zakres pierwszy danych tego zbioru: numer ewidencyjny ucznia, imię (imiona) i nazwisko, data i miejsce urodzenia, adres zamieszkania oraz imiona i nazwiska rodziców (prawnych opiekunów) ucznia – obejmuje „Księgę uczniów szkoły" i jest dostępny nauczycielowi przedmiotu głównego, dyrektorowi i jego zastępcy oraz sekretarce. Dane tego zakresu są udostępniane organowi prowadzącemu szkołę i organowi nadzorującemu szkołę w celu przeprowadzenia kontroli. Dane tego zakresu mogą być udostępnione pracownikom NIK, GIODO, MEN, MKiDN na podstawie pisemnych upoważnień do przeprowadzenia kontroli, a także policji i straży miejskiej w sytuacji popełnienia przez ucznia wykroczenia przeciw prawu.

2) Zakres drugi danych tego zbioru: imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres ich zamieszkania odnosi się do arkuszy ocen ucznia. Dane w nich zawarte przetwarzają nauczyciele przedmiotu głównego, dostęp do nich mają również dyrektor szkoły i jego zastępca oraz sekretarka, która po zakończonym cyklu kształcenia gromadzi je w specjalnych teczkach i przechowuje w archiwum szkolnym.

Dane z zakresu trzeciego mogą być udostępniane tylko przedstawicielom organu nadzorującego szkołę w celach kontrolnych.

3) Zakres trzeci danych osobowych tego zbioru: imiona i nazwisko ucznia, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres zamieszkania i numery telefonów do domu lub do pracy obejmuje dzienniki lekcyjne i jest dostępny wszystkim nauczycielom zatrudnionym w szkole. Przechowywany jest w sekretariacie w specjalnie przeznaczonej do tego celu szafce zamykanej na klucz. Nie mają do niej dostępu ani uczniowie, ani ich rodzice, jak również pozostali pracownicy szkoły, poza sekretarką, która po zakończonym roku szkolnym zdaje je do archiwum szkolnego.

Dane osobowe z tego zakresu mogą być udostępnione jedynie przedstawicielom organu prowadzącego szkołę oraz organu nadzorującego w czasie wizytacji lub w sytuacjach interwencyjnych, a także NIK i MKiDN w celu przeprowadzenia odpowiednich kontroli.

4) Zakres czwarty danych tego zbioru obejmuje dane uczniów (w tym dane wrażliwe), tj. imiona i nazwisko ucznia, data i miejsce urodzenia, adres zamieszkania, a także ostatnie dane o stanie zdrowia (w tym również zdrowia psychicznego), przedstawione w zaświadczeniach i opiniach, poradni psychologiczno-pedagogicznej.

3. Zbiór danych „Pracownicy szkoły".

Zbiór ten obejmuje dane osobowe byłych i obecnych pracowników szkoły, tj. nauczycieli, pracowników administracji i obsługi. Dane te przetwarzane są zarówno ręcznie, jak i w systemie informatycznym.

1) zakres pierwszy danych tego zbioru, tzn. imię i nazwisko nauczyciela oraz ich numery telefonów, dostępne są prawie wszystkim pracownikom szkoły, a także uczniom i ich rodzicom, jeżeli nauczyciele wyrażą na to zgodę.

2) Zakres drugi tego zbioru, tzn. imię i nazwisko pracownika szkoły, data i miejsce urodzenia imiona i nazwisko rodziców, adres zamieszkania, wysokość wynagrodzenia, dane dotyczące wynagrodzenia, kwalifikacji zawodowych, wynagrodzenia, przeszeregowań, urlopów i zwolnień lekarskich, numer dowodu osobistego, numer NIP i PESEL, a także dane wrażliwe – informacje o odbytych szkoleniach, o posiadanych dzieciach, zawartym związku małżeńskim, a także dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych na podstawie przeprowadzonych badań profilaktycznych (wstępnych, okresowych i kontrolnych) oraz w związku z ubieganiem się nauczyciela o przyznanie urlopu dla podratowania zdrowia. Dane te zamieszczone są w dokumentach teczek akt osobowych pracownika, a dostęp do nich mają:

- dyrektor szkoły,
- sekretarka, prowadząca sprawy kadrowe nauczycieli,
- kierownik gospodarczy, prowadzący sprawy kadrowe pracowników administracji i obsługi.

Dane z zakresu drugiego mogą być udostępniane organowi prowadzącemu szkołę i organowi nadzorującemu szkołę, a także innym organom prowadzącym kontrolę, w tym zwłaszcza PIP, RIO i sądom powszechnym w związku z prowadzonym postępowaniem.

W systemie informatycznym, funkcjonującym w szkole, dane zbioru „Pracownicy szkoły" są przetwarzane tylko w drugim zakresie. Na polecenie dyrektora szkoły pracownicy, zajmujący się sprawami kadrowymi, przygotowują w programie „Edytor tekstu „MS WORD" umowy o pracę, porozumienia, przeszeregowania, wypowiedzenia, w tym wypowiedzenia zmieniające, informacje o warunkach zatrudnienia, zakresy obowiązków, korespondencję w sprawie zatrudnienia i wysokości zarobków lub rozwiązania stosunku pracy i świadectwa pracy. Dane te są niezwłocznie wprowadzane do bazy danych komputera, na którym pracują te osoby. Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora i hasła pracownika, zajmującego się sprawami kadrowymi.

Z teczek akt osobowych pracowników szkoły dane są przekazywane przez osoby zajmujące się sprawami kadrowymi w sposób tradycyjny do programów SIO – system informacji oświatowej i Arkusza Optivum Vulkan – arkusza organizacyjnego i uaktualniane dwa razy do roku -31 marca i 31 września. Wprowadzanie danych do SIO jest możliwe po wprowadzeniu identyfikatora i hasła.Dostęp do tych danych mają organ prowadzący i nadzorujący szkołę, w przypadku SIO do danych osobowych ma dostęp również MEN.

4. Zbiór danych „Księgowość-finanse szkoły”.

Danymi zajmuje się Zakład Obsługi Jednostek Budżetowych.

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

1. Bezpieczeństwo osobowe.

Zachowanie poufności.

1. Dyrektor szkoły danych przeprowadza nabór na wolne stanowiska w drodze konkursu. 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 utraty bezpieczeństwa danych przetwarzanych w szkole, pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

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.

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.

2. Strefy bezpieczeństwa.

W szkole wydzielona jest jedna strefa bezpieczeństwa. Strefę stanowi sekretariat z szafą metalową, gabinet dyrektora szkoły, w których mogą przebywać inni użytkownicy danych tylko w obecności; to samo dotyczy uczniów, ich rodziców oraz interesantów; nikt z osób postronnych nie może przebywać w części sekretariatu, odgrodzonej barierką; kluczem do gabinetu dyrektora i sekretariatu może dysponować na stałe dyrektor i sekretarka po złożeniu odpowiedniego oświadczenia o konsekwencjach służbowych i dyscyplinarnych, wynikających z faktu ich zagubienia.

3. Zabezpieczenie sprzętu.

1). W celu zapewnienia większego bezpieczeństwa i ochrony danych powinno wykorzystać się system operacyjny Microsoft Windows NT/200, 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 bezpieczeństwa informatycznego jest jedyną osoba 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 sieci.

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.

4. 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 kratek 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 dyskietek;

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 szuflady 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 złożenia klucza na portierni. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów, zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym kierownika gospodarczego, który zgłasza osobie sprzątającej jednorazową rezygnację z wykonywania swej pracy. W takim przypadku także należy zostawić klucz na portierni.

5. 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 wynosić poza siedzibę administratora danych.

6. Wymiana danych i ich bezpieczeństwo.

1. Sporządzanie kopii zapasowych następuje w trybie opisanym w pkt. 8. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora bezpieczeństwa informacji oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

3. 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.

4. 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.

5. 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.

6. Należy stosować następujące sposoby kryptograficznej ochrony danych:

- przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP – tunelowanie, szyfrowanie połączenia.

7. Kontrola dostępu do systemu.

1. Poszczególnym 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 informacji po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek dyrektora szkoły, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.

2. Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora bezpieczeństwa informacji po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia, zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła.

3. 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.

8. Kontrola dostępu do sieci.

1. System informatyczny posiada szerokopasmowe połączenie z internetem. Dostęp do niego jest

jednak ograniczony. Na poszczególnych stacjach roboczych można przeglądać tylko wyznaczone strony www.

2. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

3. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie główny księgowy, upoważniony przez dyrektora szkoły, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

9. Komputery przenośne i praca na odległość.

W szkole nie używa się komputerów przenośnych do przetwarzania danych osobowych.

10. Monitorowanie dostępu do systemu i jego użycia.

1. Odpowiedzialnym za monitorowanie dostępu do systemu i jego użycia jest administrator bezpieczeństwa informacji lub upoważniona przez niego osoba, a administrator danych osobowych kontroluje jego przebieg i rezultaty.

2. System informatyczny, działający w szkole, powinien zapewnić odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu,

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,

3) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,

4) informacji o odbiorcach w rozumieniu art. 7. pkt 6. ustawy, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,

5) sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust. 1. pkt. 8. ustawy.

Odnotowanie informacji, o których mowa w pkt. 1. i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt. 1-5.

3. System informatyczny administratora danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:

1) identyfikator użytkownika;

2) datę i czas zalogowania i wylogowania się z systemu;

3) tożsamość stacji roboczej;

4) zapisy udanych i nieudanych prób dostępu do systemu;

5) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

11. 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.

12. Udostępnianie danych osobowych.

1. Udostępnianie danych osobowych policji, służbie miejskiej 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:

a) oznaczenie wnioskodawcy,

b) wskazanie przepisów uprawniających do dostępu do informacji,

c) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,

d) 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.

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

13. 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, zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

XI. 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,

zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,

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.

X. 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 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 29 listopada 2011r.