Polityka bezpieczeństwa

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W ZESPOLE PLACÓWEK OŚWIATOWYCH W KRZYWACZCE

I. POSTANOWIENIA WSTĘPNE.

1. „Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, w Zespole Placówek Oświatowych w Krzywaczce", 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 Zespole Placówek Oświatowych w Krzywaczce jak i innych osób , np. studentów, odbywających praktyki pedagogiczne.

II. DEFINICJE.

1. 1. Definicje

Ilekroć w instrukcji jest mowa o:

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

2) administratora systemu – rozumie się przez to upoważnionego pracownika sekretariatu szkoły.

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

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

5) 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,

6) osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to pracownika szkoły, który upoważniony został do przetwarzania danych osobowych przez dyrektora szkoły na piśmie,

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

8) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

9) 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.)

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

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

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

13) szkole – rozumie się przez to Zespół Placówek Oświatowych w Krzywaczce.

14) 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.)

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

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

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH.

1. 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 sieci oraz określa zakres jego 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 systemu użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,

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

W szkole funkcję administrator systemu pełni również funkcję administratora bezpieczeństwa informacji ze względów organizacyjnych i finansowych.

2. 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 danych;

8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora danych osobowych 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.

3. 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 procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

5) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. IDENTYFIKACJA ZASOBÓW SYSTEMU INFORMATYCZNEGO.

1. Struktura informatyczna Zespołu Placówek Oświatowych w Krzywaczce składa się z sieci wewnętrznej, mieszczącej się w pomieszczeniach szkoły i jest połączona siecią zbudowaną w oparciu o łącza dzierżawione w TP S.A..

2. w ramach tej struktury funkcjonuje system zainstalowany w sekretariacie szkoły. Poza tą strukturą , oddzielnie , funkcjonuje system finansowy (ZEO), za który odpowiada główny księgowy.

3. Aplikacje (sekretariatu, uczniowska) 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, Windows 7 lub Windows 10.

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 Zespołu Placówek Oświatowych w Krzywaczce. 32- 442 Krzywaczka 41.

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,

3) gabinet zastępcy dyrektora,

4) pracownia komputerowa,

5) pokój pedagoga szkolnego,

6) pokój nauczycielski,

7) pokój intendentki

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	1. Librus - sekretariat	I piętro-sekretariat	I piętro-sekretariat
2.	Uczniowie szkoły	1. Księga uczniów	I piętro - sekretariat	I piętro - sekretariat
		2. Dzienniki lekcyjne	II pietro-pokój nauczycielski	II pietro-pokój nauczycielski
		3. Arkusze ocen	I piętro - sekretariat	I piętro - sekretariat
		4. Dokumentacja medyczna	I piętro -gabinet pomocy	I piętro -gabinet pomocy

			przedmedycznej	przedmedycznej
		5. Dokumentacja pedagoga szkolnego	I piętro-pokój pedagoga	I piętro-pokój pedagoga
3.	Pracownicy szkoły	1. Akta osobowe	I piętro - sekretariat	I piętro - sekretariat
		2. SIO	I piętro - sekretariat	I piętro - sekretariat

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, 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.

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 „sekretariat”. Jest on uruchamiany przez administratora bezpieczeństwa informacji za pomocą identyfikatora i hasła. Dostęp do niego ma sekretarka. Mogą być udostępniane zarówno organowi prowadzącemu szkołę jak i organowi nadzorującemu szkołę w celu opracowywania raportów o wynikach naboru kandydatów do szkół podstawowych.

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. Ich wizerunek rejestruje program CCTV- monitoring wizyjny, do którego dostęp ma sekretariat. Może być udostępniony policji i straży miejskiej w sytuacji zaistnienia wydarzenia, będącego przedmiotem prowadzonego postępowania.

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 wychowawcom klasowym, 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 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 wychowawcy klas, 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 drugiego 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. Nie mają do nich dostępu ani uczniowie, ani ich rodzice. 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 MEN w celu przeprowadzenia odpowiednich kontroli.

4) Zakres czwarty danych zbioru „Uczniowie szkoły": imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, PESEL, informacje o przebytych chorobach, wzroście, wadze, ostrości wzroku itp., a także imiona i nazwisko rodziców (prawnych opiekunów) i ich adres zamieszkania – odnosi się do dokumentacji medycznej ucznia, na którą składają się karta zdrowia ucznia oraz wykazy ewidencyjne uczniów.

Dane z tego zakresu są przetwarzane w sposób tradycyjny przez pielęgniarkę szkolną, a dostęp do nich ma oprócz niej mają lekarz, prowadzący badania uczniów, oraz dyrektor szkoły. Wykazy ewidencyjne uczniów, w których są podane ich imiona, nazwiska oraz PESEL są przekazywane do NFZ, natomiast pozostałą dokumentację wydaje się uczniowi po zakończeniu nauki.

Dane z tego zakresu mogą być udostępnione NFZ, NIK, MZiOS na podstawie pisemnego upoważnienia w celu przeprowadzenia kontroli.

5) Zakres piąty 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, która wnioskuje do dyrektora szkoły o nauczanie indywidualne, indywidualny tok nauki, obniżenie progu wymagań albo dostosowanie warunków sprawdzianu do formy niepełnosprawności ucznia.

Dostęp do tych danych, które są przetwarzane wyłącznie ręcznie, mają wyłącznie dyrektor szkoły, jego zastępca i pedagog szkolny. Mogą być udostępnione organom, prowadzącym kontrolę, w tym zwłaszcza Kuratorium Oświaty i Okręgowej Komisji Egzaminacyjnej w Krakowie.

6) Zakres szósty danych tego zbioru: imiona i nazwisko ucznia, data i miejsce urodzenia, PESEL, adres zamieszkania, numer telefonu oraz imiona i nazwisko rodziców, dostępny jest dyrektorowi szkoły, jego zastępcy i sekretarce.

Dane te przedstawione są w wersji papierowej które następnie wprowadzane są za pomocą programu Vulkan do systemu informatycznego i przesyłane do Okręgowej Komisji Egzaminacyjnej w Krakowie w celu przetwarzania ich dla potrzeb egzaminu. Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora i hasła użytkownika, nadanych przez OKE w Krakowie.

7) Zakres siódmy danych tego zbioru dotyczy wizerunku ucznia, który rejestrują kamery, działające w programie CCTV. Dostęp do tych danych ma bezpośrednio portier i dyrektor szkoły, a także policja i służba miejska, ale tylko wtedy, jeśli prowadzi postępowanie.

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 pracownikom szkoły, 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,

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. 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".

Zakres danych tego zbioru, tzn. imię i nazwisko pracownika szkoły, jego adres zamieszkania, data i miejsce urodzenia, dane, dotyczące wykształcenia i stopnia awansu zawodowego, stażu pracy, wynagrodzenia, urlopów i zwolnień lekarskich, numeru dowodu osobistego, numeru konta bankowego, numer PESEL i NIP, dostępny jest tylko dyrektorowi szkoły i głównemu księgowymi.

Dane tego zakresu są udostępniane przez głównego księgowego ZUS-owi, urzędom skarbowym, a także firmom ubezpieczeniowym w zakresie wymaganym przez nie w tradycyjnym systemie przetwarzania danych.

Dane tego zbioru są też przetwarzane przez obsługujące ZPO w Krzywaczce – ZEO w Sułkowicach.

5) Ze względu na fakt, że system informatyczny szkoły połączony jest z siecią publiczną poprzez internet, zgodnie z §6. ust. 4. rozporządzenia MSWiA należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

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

1. 1. Bezpieczeństwo osobowe.

Zachowanie poufności.

1. Dyrektor szkoły 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 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.

3. Ryzyko ze strony osób, które dokonują bieżących napraw komputera, minimalizowane jest obecnością użytkownika systemu.

Szkolenia w zakresie ochrony danych osobowych.

1. Administrator danych 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.

3. Zabezpieczenie sprzętu.

1.Wszystkie urządzenia systemu informacyjnego w szkole są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).

2.Administrator systemu 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.

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) pilnego strzeżenia akt, dyskietek oraz dysków przenośnych;

4) kasowania po wykorzystaniu danych na dyskach przenośnych;

5) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

6) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;

7) 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;

8) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

9) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

10) 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;

11) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy;

12) niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

13) zachowania tajemnicy danych, w tym także wobec najbliższych;

14) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

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

1. Wykorzystywanie akt i dokumentów, zawierających dane osobowe (dzienniki lekcyjne, arkusze ocen), do pracy w domu jest możliwe tylko po uzyskaniu upoważnienia na piśmie, udzielanego przez dyrektora szkoły lub jego zastępcę.
2. Administrator danych lub upoważniona przez niego osoba prowadzi ewidencję akt spraw i dokumentów szkolnych, wynoszonych przez uprawnionych pracowników.
3. Niedopuszczalne jest pozostawienie akt lub dokumentów bez dozoru w czasie ich przenoszenia do domu np. w samochodzie.
4. Z wynoszonych dokumentów może korzystać wyłącznie upoważniony pracownik, który powinien dołożyć wszelkich starań, aby osoby postronne, w tym domownicy, nie mogły mieć do nich dostępu.
5. Upoważniony pracownik po zakończeniu wykonywania pracy w domu powinien niezwłocznie zwrócić dokumenty dyrektorowi szkoły lub jego zastępcy.

6. Pracownicy, wynoszący dokumenty i akta spraw do domu, są obowiązani do ochrony danych w nich zawartych i w razie ich udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym podlegają grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 zgodnie z art. 51 ustawy.

7. 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 powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki.

2) 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;

3) po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce.

8. Wymiana danych i ich bezpieczeństwo.

1. Wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora systemu.

2. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.

3. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora bezpieczeństwa informacji.

4. Administrator systemu dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń .

5. Należy stosować następujące sposoby ochrony danych:

- przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https://.

9. 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 systemu 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. .

10. Monitorowanie dostępu do systemu i jego użycia.

1. Odpowiedzialnym za monitorowanie dostępu do systemu i jego użycia jest administrator systemu.

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,

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

1. Administrator danych 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. w sytuacjach wyjątkowych w/w przegląd może być przeprowadzony częściej.

2. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora danych.

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;

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.

IX. Przeglądy polityki bezpieczeństwa.

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

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

1) zmian w budowie systemu informatycznego,

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

3) zmian w obowiązującym prawie.

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 1 września 2018 roku.