ZARZĄDZENIE Nr 4/2012/2013
DYREKTORA ZESPOŁU SZKÓŁ w RYCHLIKACH
z dnia 1.10.2015 roku

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j) Dz.U.z 2002 r. Nr 101, poz. 926 ze zm) oraz § 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

Zarządza się, co następuje:

§ 1.

Wprowadzam w Zespole Szkół w Rychlikach **Politykę Bezpieczeństwa**, której treść stanowi ***załącznik nr 1*** do zarządzenia, oraz **Instrukcję zarządzania systemem przetwarzania danych osobowych przy użyciu systemu informatycznego i w sposób ręczny**, która stanowi ***załącznik nr 2*** do zarządzenia.

§ 2.

Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią załącznika nr 1 i nr 2 do zarządzenia.

§ 3.

Oświadczenie o zapoznaniu się z treścią powyższych załączników zaopatrzone w podpis pracownika i datę, dołącza się do akt osobowych do części B. Wzór oświadczenia stanowi ***załącznik***

§ 4.

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

§ 5.

Zarządzenie wchodzi w życie z dniem ogłoszenia.

Załącznik 1 do *Zarządzenia Nr …….*
Dyrektora Zespołu Szkół w Rychlikach
z dnia ……. roku

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

I. POSTANOWIENIA WSTĘPNE

1. „Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, w Zespole Szkół w Rychlikach", 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 Szkół w Rychlikach, jak i innych, np. studentów, odbywających w nim praktyki pedagogiczne.

II. DEFINICJE

Definicje:

Ilekroć w instrukcji jest mowa o:

administratorze danych osobowych – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Zespole Szkół w Rychlikach funkcję administratora danych pełni dyrektor szkoły;

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

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

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

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

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

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 Zespół Szkół w Rychlikach;

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 pracownika szkoły upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło.

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych osobowych.

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

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,

2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, oraz odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,

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

4) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą dokumentację z zakresu ochrony danych, o ile jako właściwą do jej prowadzenia nie wskaże inną osobę,

5) zapewnia 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.

1. 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.

2. Administrator bezpieczeństwa informacji ma prawo:

1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji;

2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzanie niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;

3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;

4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;

5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.

3. Administrator systemu

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.

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 Zespołu Szkół w Rychlikach składa się z:
   1) sieci wewnętrznej, mieszczącej się w pomieszczeniach szkoły i jest połączona siecią zbudowaną w oparciu o łącza dzierżawione w NETIA SA .

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 na terenie szkoły

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

Budynek	Rodzaj dokumentów	Miejsce przechowywania

Budynek A	Dzienniki elektroniczny	Dostęp z komputerów w każdej klasie. Kazdynauczyciel ma swoje konto zabezpieczone hasłem zmienianym raz w miesiącu. Baza danych zabezpiecza firma „Vulcan”
	Dzienniki zajęć specjalistycznych	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy maswój klucz).
	Zeszyty/dzienniki wychowawcy	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy maswój klucz).
	Dzienniki zajęc pozalekcyjnych	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy maswój klucz).
	Dzienniki świetlicy	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy maswój klucz).
	Dzienniki do zajęć wg art. 42 KN	Pokój nauczycielski dostęp mają tylko nauczyciele (każdy maswój klucz).
	Dziennik pedaoga i logopedy	Pokój pedagoga – parter sala nr 10. Klucze dostępne u woznych.
	Dziennik bibliotekarza	Biblioteka szkola – piwnica sala nr13. Klucze dostępne w pokoju nauczycielskim.
	Księga ewidencji uczniów	Sekretariat szkoły – parter orazw formie elektronicznej z dostempem dla sekretarza szkoły.
	Księga uczniów	Sekretariat szkoły – parter orazw formie elektronicznej z dostempem dla sekretarza szkoły.
	Arkusze ocen	Sekretariat szkoły – parter orazw formie elektronicznej z dostempem dla sekretarza szkoły.
	Dokumenty z nadzoru pedagogi cznego	Gabinet dyrektora szkoły – parter Klucze dostępne na portierni
	Dokumentacja pomocy pp	Gabinet dyrektora szkoły – parter oraz pokój pedagoga – parter
	Ewidencja uczniów przystępujących do sprawdzianu/egzaminu zewnętrznego	Sekretariat szkoły – parter.
	Dokumentacja opiekuńczo-wychowawcza	Gabinet dyrektora szkoły – parter pedagoga szkolnego – parter
	Arkusz organizacyjny szkoły	Sekretariat szkoły – parter.
	Dokumentacja ZFŚS	Gabinet dyrektora szkoły – parter
	Postępowanie administracyjne w sprawie realizacji obowiązku nauki	Sekretariat szkoły – parter.
	Decyzje o odroczenie obowiążku szkolnego	Sekretariat szkoły – parter.
	Podania ubiegających się o pracę	Sekretariat szkoły – parter.
	Ewidencja wydanych świadectw, zaświadaczeń i legitymacji	Sekretariat szkoły – parter.
	Księga kontroli zewnętrznej	Sekretariat szkoły – parter.
	Lista obecności	Sekretariat szkoły – parter.
	Dziennik korespondencyjny	Sekretariat szkoły – parter.
	Rejestr upoważnień	Sekretariat szkoły – parter.
	protokóły wypadkowe	Sekretariat szkoły – parter.
	Dokumenty archiwalne	Archiwum - Klucze w sekretariacie.
	Lokalne bazy SIO – uczniowie i budynki	Sekretariat szkoły – parter.
	Teczki awansu zawodowego	Sekretariat szkoły – parter.
Budynek A	Akta osobowe	Sekretariat szkoły – parter.
	Listy płac	Pokój głównej księgowej i referenta – p.
	Dokumentacja Komisji Zdrowotnej	Sekretariat szkoły – parter.

	Dokuementacja kadrowa	Pokój głównej księgowej i referenta – p.
	Lokalne bazy SIO - sprawy kadrowe	Sekretariat szkoły – parter.

Opis pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe

1. Zespół Szkół mieści się w budynkach 34 w Rychlikach, są tu: sekretariat i pokój dyrektora o numerze .
2. Sekretariat i pokój dyrektora znajduje się na parterze i każdy jest przystosowany do pracy dla jednej osoby, zajmują je sekretarka szkoły oraz dyrektor, w pokojach tych przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. płyty CD przechowuje się w szafach zamykanych na klucze, które są w posiadaniu dyrektora i sekretarki szkolnej. Komputer (laptopy) zasilane baterią umożliwiają prawidłowe zamknięcie systemu komputerowego w razie spadku lub braku prądu. W komputerze znajduje się program SIO – system informacji oświatowej. Program może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
3. Pokój nauczycielski znajduje się na parterze budynku B. W pokoju tym przetwarzane są dane osobowe uczniów i ich rodziców ręcznie. Dokumentację papierową przechowuje się podczas zajęć dydaktycznych w szafach z przegródkami w pokoju nauczycielskim, natomiast po zakończeniu zajęć w szafce zamykanej na klucz, do której dostęp mają woźni szkolni.
4. Pokój pedagoga szkolnego znajduje się na parterze budynku B i przystosowany jest do pracy dla jednej osoby. W pokoju tym przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. płyty CD przechowuje się w szafach zamykanych na klucze, które są w posiadaniu pedagoga. Komputer może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
5. Biblioteka szkolna znajduje się w budynku B.. Do przeglądu zapisu ma dostęp bibliotekarka szkolna, woźny oraz dyrektor szkoły. Odtwarzanie nagrania można uruchomić poprzez wprowadzenie hasła. Nagranie z monitoringu wizyjnego można kopiować na płyty CD, które zabezpiecza dyrektor szkoły.
6. W pomieszczeniu nr 15 znajduje się rejestrator monitoringu CCTV. Urządzenie podłączone jest do UPS podtrzymującego energię elektryczną. Zapis danych odbywa się automatycznie i jest przechowywany przez urządzenie przez 30 dni, po tym terminie zapis jest samoczynnie kasowany Do przeglądu zapisu ma dostęp dyrektor szkoły. Odtwarzanie nagrania można uruchomić poprzez wprowadzenie hasła. Nagranie z monitoringu wizyjnego można kopiować na płyty CD, które zabezpiecza dyrektor szkoły.
7. Świetlica szkolna znajduje się w piwnicy budynku szkolnego nr 12. W pomieszczeniu przechowuje się dziennik zajęć świetlicy w biurku nauczycielskim, w szufladzie zamykanej na klucz, który posiadają wychowawcy świetlicy.

8. Pieczęcie z nazwą i siedzibą instytucji oraz imienne są przechowywane w szafie pancernej Zespołu Szkół w Rychlikach, które otwiera i zamyka sekretarka szkoły lub dyrektor.
9. Przesyłki zawierające dane osobowe przesyła się jako polecone z ewentualnym zwrotnym potwierdzeniem odbioru oraz zabezpieczone w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby nieupoważnione .
10. Dokumenty zawierające dane osobowe przekazuje się do archiwum mieszczącego się w Zespole Szkół w Rychlikach, po okresie przydatności dokumenty zawierające dane osobowe niszczy się na podstawie decyzji dyrektora komisyjnie, w warunkach gwarantujących zabezpieczenie danych osobowych w sposób gwarantujący uniemożliwienie ich odtworzenia, wykazy i spisy zdawczo - odbiorcze dokumentów zawierające dane osobowe przekazywanych do archiwum oraz protokoły zniszczenia dokumentów przechowuje administrator danych. Dostęp do archiwum szkolnego posiada sekretarka szkolna oraz dyrektor szkoły.
11. Dokumenty zawierające dane osobowe niezbędne do pracy w terenie należy przechowywać w warunkach gwarantujących ich należytą ochronę.
12. Dane osobowe pracowników Zespołu Szkół w Rychlikach są również przetwarzane w budynku Urzędu Gminy Rychliki.

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

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. Windows	parter-sekretariat	parter-sekretariat
		2. CCTV	Korytarze szkolne i na budynkach szkolnych	Sala nr 15
2.	Uczniowie szkoły	1. Księga uczniów	parter-sekretariat	parter-sekretariat
		2. Dzienniki lekcyjne elektroniczny	Komputer w każdej klasie (zabezpieczony hasłem i programem antywrusowym „Kaspersky”	Gabinety zajęć lekcyjnych
		3. Arkusze ocen	parter-sekretariat	Pokój nauczycielski
		4. SIO	parter - sekretariat	parter – sekretariat i Urząd Gminy Rychliki
		5. Dokumentacja pedagoga szkolnego	parter-pokój pedagoga	parter-pokój pedagoga
		6. Dokumentacja	pokój	Gabinety zajęć

		wychowawcy klasy	nauczycielski	lekcyjnych
		7. HERMES	Parter sekretariat	parter-sekretariat
		8. CCTV	Korytarze szkolone, na budynkach szkolnych	parter-sala nr 15
3.	Pracownicy szkoły	1. Akta osobowe	Parter- sekretariat	parter-sekretariat
		2. SIO	parter-sekretariat, Urząd Gminy –	Urząd Gminy – parter-sekretariat
		3. Edytor tekstu	parter-sekretariat,	parter-sekretariat,
		4. CCTV	Korytarze szkolne, na budynkach szkolnych	Sala nr 15
4.	Księgowość-finanse szkoły	1. program KADROWO-PŁACOWY	Parter - księgowość	Parter - księgowość
		2. Płatnik ZUS	Parter - księgowość	Parter - księgowość

2. WYKAZ PROGRAMÓW STOSOWANYCH W SZKOLE:

- Windows
- Linux,
- Office,
- Libre office
- HERMES,
- SIO- System Informacji Oświatowej,
- CCTV – monitoring wizyjny,
- Program KADROWO-PŁACOWY,
- Płatnik- program obsługujący przelewy danych do ZUS.

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

KARTY ZBIORÓW

Lp.	Nazwa zbioru (dokumentu) - opis	Podstawa prawna przetwarzania	Struktura zbioru	Program	dostęp
1.	Księga Ewidencji - Coroczna adnotacja o spełnianiu przez dziecko obowiązku szkolnego w tej albo innej szkole	§ 3b.2. pkt 1) rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r, z późn. zm.)	Imię (imiona) i nazwisko, datę i miejsce urodzenia oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania, PESEL		Dyrektor, zastępca, sekretarka
2.	Karta zapisu dziecka do szkoły - Informacje dot.	§ 4.1. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres	WINDOWS Edytor	Dyrektor, zastępca, sekretarka

	ucznia przyjmowanego do szkoły	przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	zamieszkania lub pobytu, PESEL, wizerunek dziecka, wynik sprawdzianu szóstoklasisty, wyniki edukacyjne na świadectwie, telefon	tekstu	
3.	Księga Uczniów - Zbiór danych o uczniach	§ 4.1. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, przyjęcie do szkoły: data, klasa, obwód szkolny. Wypisanie ze szkoły: data, klasa, powody, data wydania dok, ukończenia szkoły numer wydanego świadectwa.		wychowawcy dyrektor, zastępca, sekretarka (kontrola: organ prowadzący i organ nadzoru, NIK, GIODO, MEN))
4.	Dziennik lekcyjny elektroniczny - Dokumentacja przebiegu nauczania w danym roku szkolnym	§ 7.2. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL		Nauczyciele, praktykanci, sekretarka (kontrola: organ prowadzący i nadzoru, NIK, MEN)
5.	Arkusz Ocen - dokumentacja wyników nauczania ucznia w poszczególnych latach	§ 12.1. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.) art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, nr księgi uczniów, przebieg nauki, wyniki nauki		wychowawcy dyrektor, zastęca, sekretarka (kontrola: organ nadzoru)
6.	Ewidencja świadectw szkolnych	§ 5.2 Rozporządzenia Ministra Edukacji Narodowej z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych	Nazwiska i imiona, PESEL		Dyrektor, zastępca, sekretarka, wychowawcy
7.	Ewidencja legitymacji szkolnych i kart motorowerowych	§ 5.2 Rozporządzenia Ministra Edukacji Narodowej z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych	Nazwiska, imiona, PESEL		Dyrektor, zastępca, sekretarka

8.	Księga arkuszy ocen - zbiór arkuszy ocen uczniów urodzonych w jednym roku, którzy ukończyli lub opuścili szkołę	§ 13.1. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Nr księgi uczniów, przebieg nauki, wyniki nauki		Dyrektor, zastępca, sekretarka
9.	Protokoły Rady Pedagogicznej	§ 16 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.) art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, data urodzenia, stan zdrowia, przebieg nauki, wyniki nauki, pomoc psycholog.-pedagogiczna		Nauczyciele, dyrektor, zastępca (kontrola: organ prowadzący i nadzoru, MEN)
10.	Okręgowa Komisja Egzaminacyjna	Art. 41.1 pkt 1) Rozporządzenia Ministra Edukacji Narodowej z dnia 30 kwietnia 2007 r. w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów i słuchaczy oraz przeprowadzania sprawdzianów i egzaminów w szkołach publicznych (Dz.U. Nr 83 poz.562 z późn. zm.)	Nazwisko, imiona, data i miejsce urodzenia, PESEL, płeć, dysleksja, wyniki nauki	Hermes	Dyrektor, zastępca, nauczyciele
11.	Stypendia	art. 90f, 90g ustawy z dnia 7 września 1991 r. o systemie oświaty	Imię, nazwisko, data urodzenia, adres zamieszkania, PESEL, imiona i nazwiska rodziców, adresy zamieszkania, dochody	WINDOWS Edytor tekstu	Dyrektor, zastępca, sekretarka, wychowawcy nauczyciele, GZEAS
12.	Wyprawka szkolna	Rozporządzenie Rady Ministrów Rady Ministrów w sprawie szczegółowych warunków udzielania pomocy finansowej uczniom na zakup podręczników oraz wypłaty uczniom zasiłku powodziowego na cele edukacyjne	Nazwisko, imię ucznia, data urodzenia, miejsce urodzenia, adres zamieszkania, imiona i nazwiska rodziców, adres zamieszkania, dochód	WINDOWS Edytor tekstu	Dyektor, zastępca, sekretarka, GZEAS
13.	Karty biblioteczne	art. 67.1 pkt 2) ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwisko, imię, adres zam., dane o wypożyczeniach		Dyrektor, zastępca, bibliotekarz

14.	Dziennik Pedagoga –Dziennik zawiera informacje o uczniach zakwalifikowanych do różnych form pomocy	§ 18 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, Informacje o kontaktach z innymi osobami, instytucjami, stan zdrowia		Dyrektor, zastępca, wychowawcy pedagog, logopeda, nauczyciele
15.	Dokumentacja pomocy psycholog.-pedagogicznej w szkole – Dokumentacja badań i czynności uzupełniających prowadzonych przez nauczycieli i pedagoga	§ 19 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.) art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Różne dane niezbędne do dokumentowania przebiegu terapii, nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia, opinia PPP	WINDOWS Edytor tekstu	Dyrektor, zastępca, wychowawcy pedagog, logopeda, nauczyciele, sekretarka
16.	Dziennik zajęć rewalidacyjno – wychowaw. Dokumentacja przebiegu zajęć z uczniami upośledzonymi umysłowo.	§ 11 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu		Dyrektor, zastępca, pedagog, nauczyciele, sekretarka
17.	Lista uczestników wycieczek	§ 7.3 pkt 5 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 8 listopada 2001 r. w sprawie warunków i sposobu organizowania przez publiczne przedszkola, szkoły i placówki krajoznawstwa i turystyki.	Nazwisko i imię, wiek, data urodzenia, adres zamieszkania, PESEL	WINDOWS Edytor tekstu	Dyrektor, zastępca, sekretarka, nauczyciele
18.	Ubezpieczenie uczniów	Zgoda osób	Imiona nazwiska, adres zamieszkania lub pobytu		Dyrektor, zastępca, sekretarka
19.	Dokumentacja wypadków uczniów - Informacje o wypadkach uczniów	§ 43.3 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach.	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia		Dyrektor, zastępca, sekretarka, wychowawcy nauczyciele
20.	Opinie i Orzeczenia Poradni Psychologiczno-Pedagogicznej	Rozporządzenia Ministra Edukacji Narodowej z dnia 17 listopada 2010 r. w sprawie zasad udzielania i organizacji pomocy psychologiczno-pedagogicznej w publicznych	Imię i nazwisko, data urodzenia, stan zdrowia		Dyrektor, zastępca, wychowawcy pedagog, logopeda,

		przedszkolach, szkołach i placówkach (Dz. U. z 2010 r., Nr 228, poz. 1487)			nauczyciele, sekretarka
21.	Wnioski rodziców o naukę religii i etyki	§ 1.1 pkt 1 rozporządzenia Ministra Edukacji Narodowej z dnia 14 kwietnia 1992 r. w sprawie warunków i sposobu organizowania nauki religii w publicznych przedszkolach i szkołach (tekst jednolity Dz. U. 1993 nr 83 poz. 390)	Imię, nazwisko dziecka oraz imiona i nazwiska rodziców i adresy zamieszkania, przynależność wyznaniowa		Dyrektor, zastępca, sekretarka, wychowawcy
22.	Zwolnienia lekarskie uczniów z wychowania fizycznego – decyzje dyrektora szkoły	Rozdział 2, § 8, ust., 2 Rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 30 kwietnia 2007 r. w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów i słuchaczy oraz przeprowadzania sprawdzianów i egzaminów w szkołach publicznych	Imię i nazwisko, rodzaj schorzenia lub choroby	WINDOWS Edytor tekstu	Dyrektor, zastępca, sekretarka, wychowawcy nauczyciele w-f
23.	Dziennik zajęć pozalekcyjnych i nauczania indywidualnego	§ 10 Rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Imię i nazwisko, adres zamieszkania		Dyrektor, zastępca, sekretarka, wychowawcy nauczyciele
24.	Zgody na przetwarzanie danych	Zgoda osób	Imię i nazwisko adres udzielającego zgodę		Dyrektor, zastępca, sekretarka, wychowawcy nauczyciele
25.	Ewidencja wejść do placówki	Zgoda osób	Nazwisko, imię		Dyrektor, zastępca, sekretarka, woźny
26.	Akta osobowe - Zbiór zatrudnionych pracowników	Art. 22 oraz 229 § 7 ustawy z dnia 26.06.1974 Kodeks pracy	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, wykształcenie, przebieg dotychczasowego zatrudnienia, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia	Program kadrowo-płacowy	Dyrektor, zastępca, sekretarka, księgowa,

27.	System Informacji Oświatowej Zbiór zawiera informacje o nauczycielach i uczniach szkoły	Ustawa o systemie informacji oświatowej (Dz. U. z 2011 r. Nr 139, poz. 814)	PESEL, miejsce pracy, zawód, wykształcenie, wynagrodzenie	SIO	Dyrektor, zastępca, sekretarka, księgowa,
28.	Komisja Socjalna - Świadczenia dla pracowników	Art. 8 ust. 2 ustawy z dnia 4.03.1994 o zakładowym funduszu świadczeń socjalnych	Nazwiska i imiona, adres zamieszkania lub pobytu, stan zdrowia	WINDOWS Edytor tekstu	Dyrektor, zastępca, sekretarka, Nauczyciele z komisji, księgowa,
29.	Dobrowolne ubezpieczenie pracowników	Zgoda osób	Imiona nazwiska, adres zamieszkania lub pobytu, PESEL, nr telefonu		Dyrektor, zastępca, sekretarka, księgowa,
30.	Dokumentacja wypadków pracowników - Informacje o wypadkach pracowników	§ 1.2 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 19 grudnia 2002 r. (Dz. U. Nr 236, poz. 1992) § 4.1 Rozporządzenia Ministra Gospodarki i Pracy z 16.9.2004 r. w sprawie wzoru protokołu ustalenia okoliczności i przyczyn wypadku przy pracy - Dz. U. Nr 227, poz. 2298	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, stan zdrowia	WINDOWS Edytor tekstu	Dyrektor, zastępca, sekretarka, Służba BHP
31.	Listy płac pracowników		Nazwiska i imiona, poszczególne składniki wynagrodzenia	Program kadrowo-płacowy Program Płatnik	Dyrektor, zastępca, sekretarka, księgowa,
32.	Umowy zlecenia	Art. 734 – 751 ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz. U. z dnia 18 maja 1964 r.)	Nazwiska i imiona, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu	WINDOWS Edytor tekstu	Dyrektor, zastępca, sekretarka, księgowa,
33.	Przelewy	Ustawa o rachunkowości	Nazwiska, imiona, adresy zamieszkania, nr kont bankowych kontrahentów będących osobami fizycznymi, NIP, wyciągi bankowe	Program Płatnik	Dyrektor, zastępca, sekretarka, księgowa,

34.	Faktury	art. 23.1 pkt 3 ustawy o ochronie danych osobowych	Nazwisko, imię, adres zamieszkania	Program Płatnik	Dyrektor, zastępca, kięgowa, sekretarka,
35.	Książka korespondencyjna	1.Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tekst jednolity Dz. U. z 2006 r. Nr 97, poz. 673 z późn. zm.) 2. Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. 2002, Nr 167, poz. 1375)	Imię i nazwisko, adres zamieszkania		Dyrektor, zastępca, sekretarka,
36.	Kasa zapomogowo-pożyczkowa	art. 39 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. Nr 55 poz. 234), Rozporządzenie RM z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych w zakładach pracy (Dz. U. Nr 100 poz. 502 z późn. zm.) oraz § 7.1 Rozporządzenia Rady Ministrów z dnia 19 grudnia 1992 w sprawie pracowniczych kas zapomogowo pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy (Dz. U 100 poz. 502)	Nazwiskoi imię, data urodzenia, miejsce zamieszkania, imię i nazwisko oraz adres zamieszkania osoby uposażonej do odebrania świadczeń na wypadek śmierci, dane osobowe poręczycieli, wysokości pożyczki.		Zarząd KZP Kasier Księgowa
37.	Awans zawodowy	Art. 9 a, 9 b ust 1 pkt 2ustawy z dnia 26 stycznia 1982 rok -Karta Nauczyciela (Dz. U. z 2006, Nr 97 poz. 674 z późn. zm.)	Imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zam., przebieg zatrudnienia, wykształcenie, składniki wynagrodzenia, zapytanie o karalność, stan zdrowia	WINDOWS Edytor tekstu	Dyrektor, zastępca, sekretarka,

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

1. Bezpieczeństwo osobowe.

Zachowanie poufności.

1. Dyrektor szkoły przeprowadza nabór na wolne stanowiska w drodze oferty. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia szkolne), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń – zakres obowiązków pracownika.

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

Szkolenia w zakresie ochrony danych osobowych.

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

Strefy bezpieczeństwa.

W szkole wydzielono dwie strefy bezpieczeństwa. Do strefy I wchodzą:

1) gabinet księgowej pokój nr …. w którym może przebywać główny księgowy, referent; inni użytkownicy danych (sekretarka i nauczyciele) tylko w towarzystwie głównej księgowej, a osoby postronne w ogóle nie mają dostępu;

2) sekretariat z kasą pancerną, gabinet dyrektora szkoły, w których mogą przebywać inni użytkownicy danych tylko w obecności ww. wymienionych; to samo dotyczy uczniów, ich rodziców oraz interesantów; nikt z osób postronnych nie może przebywać w części sekretariatu, odgrodzonej zabudowanym modułem; 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.

W strefie II do danych osobowych mają dostęp wszystkie osoby upoważnione do ich przetwarzania, a osoby postronne (uczniowie, ich rodzice i praktykanci) tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje pokój nauczycielski, bibliotekę szkolną, świetlicę szkolną i pokój pedagoga szkolnego.

3. Zabezpieczenie sprzętu.

1. Komputery w sekretariacie, rejestrator monitoringu wizyjnego oraz komputery w księgowości są zabezpieczone programem antywirusowym.
2. W celu zapewnienia większego bezpieczeństwa i ochrony danych powinno wykorzystać się system operacyjny Microsoft Windows, posiadający rozbudowane mechanizmy nadawania uprawnień i praw dostępu. Dla pełnego wykorzystania mechanizmów należy

stosować system plików NTFS, który zapewnia wsparcie mechanizmu ochrony plików i katalogów oraz mechanizmów odzyskiwania na wypadek uszkodzenia dysku lub awarii komputerów.

3.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.

4. Bieżąca konserwacja sprzętu wykorzystywanego w szkole do przetwarzania danych prowadzona jest przez jej pracowników, przede wszystkim przez administratora sieci.

5. 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.

6. 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.

7. 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 nośników komputerowych;
6) kasowania po wykorzystaniu danych na dyskach przenośnych;
7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;
8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;

11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
12) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;
13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
16) kończenia pracy stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;
17) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy;
18) niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
19) zachowania tajemnicy danych, w tym także wobec najbliższych;
20) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
21) umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
22) zamykanie okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
23) zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza na portierni. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów, zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym dyrektora szkoły, który zgłasza osobie sprzątającej jednorazową rezygnację z wykonywania swej pracy. W takim przypadku także należy zostawić klucz na portierni.

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

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

6. Postępowanie z nośnikami danych i ich bezpieczeństwo.

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

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

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

7. Wymiana danych i ich bezpieczeństwo.

1. Sporządzanie kopii zapasowych następuje w trybie opisanym w pkt. 9. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. 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,

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

8. 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.

9. 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. 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.

10. Komputery przenośne i praca na odległość.

W szkole używa się komputerów przenośnych (komputer dyrektora szkoły) do przetwarzania danych osobowych, które uruchamia się po wprowadzeniu hasła.

11. 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

12. 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.

13. Udostępnianie danych osobowych.

1. Udostępnianie danych osobowych policji i sądom może nastąpi w związku z prowadzonym przez nie postępowaniem .

2. Udostępnianie informacji policji odbywa się według następującej procedury:

1) udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:

- oznaczenie wnioskodawcy,
- wskazanie przepisów uprawniających do dostępu do informacji,
- określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,

- wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

2) udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

3) osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.

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

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

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

14. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
Niezależnie od rozwiązania stosunku pracy osoby, popełniające przestępstwo, będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51 i 52. ustawy oraz art. 266. Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

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

IX. Przeglądy polityki bezpieczeństwa i audyty systemu.

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

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

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

Administrator bezpieczeństwa informacji po uzgodnieniu z dyrektorem szkoły może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji, jak i dyrektora.

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

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 1.10.2012 r.

4. Traci moc polityka bezpieczeństwa, wprowadzona w życie zarządzeniem nr 11/2008/2009 dyrektora szkoły z dnia 16 marca 2009 r.

Rychliki, 1.10.2015 ***Dyrektor Zespołu Szkół w Rychlikach***

__Załącznik 2__ do Zarządzenia Nr 4/2012/2013
Dyrektora Zespołu Szkół w Rychlikach
z dnia 1.10.2012 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ W TRZEBIELU

I. CELE WPROWADZENIA I ZAKRES ZASTOSOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM.

1. „Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Zespole Szkół w Rychlikach", zwana dalej instrukcją, została wprowadzona w celu spełnienia wymagań, o których jest mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r., nr 101, poz. 926. z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U. 2004 r., nr 100, poz. 1024), tj. zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Zespole Szkół w Trzebielu" i wraz z nim składa się na dokumentację wymaganą przez art. 36. ust. 2. ustawy o ochronie danych osobowych.

3. Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w szkole, w których są przetwarzane dane osobowe.

4. Instrukcja podlega monitorowaniu i w razie potrzeby uaktualnianiu co roku, do końca stycznia, przez administratora danych osobowych lub upoważnioną przez niego osobę, w ramach sprawowania kontroli zarządczej.

5. Dokument instrukcji przechowywany jest w wersji papierowej i elektronicznej.

II. DEFINICJE.

1. Definicje

Ilekroć w instrukcji jest mowa o:

1) **administratorze danych osobowych** – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Zespole Szkół Rychliki funkcję administratora danych pełni dyrektor szkoły;
2) **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji (ABI);
3) **administratorze systemu** – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagane specjalnych uprawnień;
4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) **zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;
6) **przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywania, udostępnianie, zmienianie, usuwanie;
7) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
8) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
9) **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,
10) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to pracownika szkoły, która upoważniona została do przetwarzania danych osobowych przez dyrektora szkoły na piśmie;
11) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
12) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
13) **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.);
14) **serwisancie** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;
15) **sieci publicznej** – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
16) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
17) **szkole** – rozumie się przez to Zespół Szkół w Rychlikach;
18) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci

telekomunikacyjnej;

19) **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.);

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

21) **użytkowniku** – rozumie się przez to pracownika szkoły upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło.

III. NADAWANIE I REJESTROWANIE (WYREJESTROWANIE) UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM.

1. Nadawanie i rejestrowanie uprawnień.

1) Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez dyrektora szkoły lub uprawnioną przez niego osobę.

2) Rejestracja użytkownika, o którym jest mowa w pkt. 1., polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

2. Wyrejestrowanie uprawnień.

1) Wyrejestrowanie użytkownika systemu informatycznego dokonuje dyrektor szkoły lub upoważniona przez niego osoba.

2) Wyrejestrowanie, o którym jest mowa w pkt. 1., może mieć charakter czasowy lub trwały.

3) Wyrejestrowanie następuje przez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4) Czasowe wyrejestrowanie użytkownika z systemu musi nastąpić w razie:
   a) nieobecności użytkownika w pracy, trwającej dłużej niż 21 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych.

5) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   a) wypowiedzenie umowy o pracę,
   b) wszczęcie postępowania dyscyplinarnego.

6) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

IV. METODY I ŚRODKI UWIERZYTELNIENIA.

1. Każdy użytkownik systemu informatycznego otrzymuje od administratora bezpieczeństwa informacji identyfikator i hasło.

2. Identyfikator składa się z sześciu znaków, z których dwa pierwsze odpowiadają dwóm pierwszym literom imienia użytkownika, a cztery kolejne- czterem pierwszym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne./ wpisać własne/

3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika systemu administrator bezpieczeństwa informacji nadaje inny identyfikator, odstępując od zasady określonej w pkt. 1.

4. Hasło użytkownika powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

5. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

6. Zmiana haseł w systemie następuje nie rzadziej niż co 30 dni.

V. PROCEDURY ZWIĄZANE Z GROMADZENIEM, PRZECHOWYWANIEM, PRZETWARZANIEM, USUWANIEM DANYCH OSOBOWYCH.

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informacyjnym oraz wskazanie osoby odpowiedzialnej za te czynności.

1) Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych (wzór tego upoważnienia stanowi załącznik do zarządzenia dyrektora szkoły). Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego, przetwarzającego dane osobowe, następuje na wniosek dyrektora szkoły.

2) Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia upoważnienia zostaje dołączona do akt osobowych pracownika.

3) Identyfikator i hasło do systemu informatycznego, przetwarzającego dane osobowe, są przydzielone użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator bezpieczeństwa informatycznego. Wyrejestrowanie użytkownika z systemu informatycznego następuje na wniosek administratora danych osobowych.

4) Administrator jest zobowiązany do przeprowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Zespole Szkół w Trzebielu.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła
.
2) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.

3) Identyfikator i hasło użytkownika powinny odpowiadać wymaganiom, określonym w rozdziale IV.

4) Nazwy i hasła użytkowników, posiadających uprawnienia do informatycznego przetwarzania danych osobowych, powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do nich mają wyłącznie osoby uprawnione. Nazwy i hasła użytkowników powinny być przechowywane w opieczętowanej i opatrzonej pieczęcią szkoły i podpisem administratora w kopercie.

5) W przypadku konieczności użycia nazw i haseł tych użytkowników konieczny jest wpis, ilustrujący zaistniałą sytuację w „Dzienniku haseł", który jest przechowywany w sejfie lub wraz z kopertą, w której znajdują się hasła. Wpis powinien zawierać następujące informacje:

a) imię i nazwisko oraz stanowisko osoby upoważnionej, udostępniającej dostęp do szafy, w której znajdują się hasła,

b) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
c) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

6) O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie
zostać powiadomiony administrator bezpieczeństwa informacyjnego.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy, mogące świadczyć o naruszeniu ochrony danych osobowych.

2) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3) Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem bezpieczeństwa informacji. Użytkownik informuje administratora bezpieczeństwa informacji o zablokowaniu dostępu do zbioru danych.

4) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączony jest wygaszasz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.

5) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.

6) W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut, użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje, oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji, zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

7) Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania.

1) Dane osobowe, przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie w tym celu wyznaczona.

2) Kopie zapasowe informacji przechowywanych w systemie informatycznym, przetwarzającym dane osobowe, tworzone są w następujący sposób:

a) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w zamkniętej szafie,
b) kopia zapasowa danych osobowych przetwarzanych przez aplikację (pełna kopia) wykonywana jest codziennie na dysku komputera wybranego przez administratora systemu informatycznego,
c) zbiorcze (tygodniowe) kopie przechowywane są przez okres dwóch tygodni, po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne.

3) W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego, przetwarzającego dane osobowe, których to dotyczy, muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego lub osoba przez niego upoważniona.

4) Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych danych.

4. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

1) Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

2) Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynek szkoły powinno odbywać się za wiedzą administratora bezpieczeństwa informacji.

3) W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie 4. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

4) W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej
zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje.

6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1) W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.

2) Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji, umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania
  danych z wykorzystaniem ogólnodostępnej sieci internet,
- przechwycenie danych z aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany
  program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania
  danych,

- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy, zakłócający pracę aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

3) W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

- autoryzację użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

Ponieważ systemy informatyczne, działające w szkole, nie są połączone z serwerem, nie ma konieczności stosowania rygorystycznego systemu autoryzacji dostępu do nich oraz stosowania aplikacji i nieumieszczania kodu źródłowego aplikacji na serwerach.

4) Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje, pochodzące z nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.

5) W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego, przetwarzający dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem, wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor, zapewniający ochronę przed wirusami w dokumentach MS Office, powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

6) Systemy antywirusowe, zainstalowane na stacjach roboczych, powinny być skonfigurowane w sposób następujący:

- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

7) System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

8) Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

- skanowania zawartości dysków stacji roboczej, pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej 2 razy w tygodniu,
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej, pracującej w systemie informatycznym, pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

9) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania, zmierzające do usunięcia zagrożenia.

W szczególności działania te mogą obejmować:

- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowefunkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

10) System informatyczny, przetwarzający dane osobowe, powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku
awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny
powinien być wyposażony w co najmniej:

- filtry zabezpieczające stacje robocze przed skutkami przepięcia,

7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1. pkt. 4. rozporządzenia MSWiA.

1) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy, pozwalające na określenie uprawnień użytkownika do korzystania
z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych,
tworzenia nowych danych, usuwania danych).

2) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizmy, pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom niebędącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego, przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3) Zapis działań użytkownika uwzględnia:

- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

4) Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego, przetwarzającego dane osobowe, muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

2) Prace serwisowe na terenie szkoły, prowadzone w tym zakresie, mogą być wykonywane wyłącznie przez jego pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych, znajdujących się w towarzystwie pracowników szkoły.

3) Przed rozpoczęciem prac serwisowych przez osoby spoza szkoły konieczne jest potwierdzenie tożsamości serwisantów.

4) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VI. POZIOM BEZPIECZEŃSTWA

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6. rozporządzenia.

VII. STOSOWANE ŚRODKI BEZPIECZEŃSTWA

1. Zgodnie z treścią § 6. ust. 4 rozporządzenia o którym jest mowa w pkt. 1.1. niniejszej instrukcji stosuje się w szkole środki bezpieczeństwa na poziomie wysokim.

2. W szkole stosuje się następujące środki bezpieczeństwa:

1) Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2) Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3) Stosowane są mechanizmy kontroli dostępu do danych.

4) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.

5) W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

6) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów, służących do przetwarzania danych osobowych.

7) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.

8) Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

9) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

10) W przypadku, gdy do uwierzytelnienia użytkowników używa się haseł, hasło to składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

11) Urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

12) Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

VIII. POSTANOWIENIA KOŃCOWE.

1. Osobą odpowiedzialną za przegląd przestrzegania instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu

informatycznego jest administrator bezpieczeństwa informacji lub inna osoba upoważniona przez administratora danych.

2. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie (załącznik nr 5), potwierdzające znajomość jej treści.

4. Niezastosowanie się do procedur określonych w niniejszej instrukcji 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.

5. Niniejsza instrukcja wchodzi w życie z dniem 1.10.2015 r.

Rychliki, 1.10.2015 ***Dyrektor Zespołu Szkół w Rychlikach***
(Administrator danych osobowych)

Załącznik nr 1. Wzór oświadczenia pracownika dotyczącego ochrony danych osobowych

.....
(data)

.....
(imię i nazwisko pracownika)

Oświadczenie pracownika

zatrudnionego przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez Zespół Szkół w Rychlikach

Obowiązki pracownika

Pracownik dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

1. Zapoznania się i przestrzegania obowiązków wynikających z:
   a. Przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz aktów wykonawczych wydanych na jej podstawie,
   b. Dokumentów wprowadzonych przez Dyrektora Zespołu Szkół w Rychlikach w związku z przetwarzaniem danych osobowych, w szczególności:
      - Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
      - Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych
2. Zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.
3. Zachowania w tajemnicy danych oraz sposobu ich zabezpieczenia, do których uzyskał dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

Odpowiedzialność pracownika

Za niedopełnienie obowiązków wynikających z niniejszego oświadczenia pracownik ponosi odpowiedzialność na podstawie przepisów Regulaminu Pracy, Kodeksu Pracy oraz Ustawy o ochronie danych osobowych.

Oświadczam, że treść niniejszego oświadczenia jest mi znana i zobowiązuję się do jego przestrzegania.

Potwierdzam odbiór 1 egz. oświadczenia.

....

pracownik pracodawca

Załącznik nr 2. Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podst. na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.)
- udziela się Pani/Panu[1]:

……..
(imię i nazwisko pracownika)

……
(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych, których Administratorem jest Zespół Szkół w Rychlikach oraz do przetwarzania danych osobowych powierzonych szkole przez podmioty trzecie.
Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań oraz polecenia służbowego.
Upoważnienie traci moc z chwilą ustania stosunku pracy.

……..
(data i podpis Administratora Bezpieczeństwa Informacji)

[1] Niepotrzebne skreślić

Zał. Nr ….

do instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Zespole Szkół w Rychlikach

EWIDENCJA OSÓB UPOWAŻNIONYCH

WYKAZ UŻYTKOWNIKÓW I ICH UPRAWNIEŃ W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

L.p	Nazwa zbioru danych	Nazwisko i imię osoby upoważnionej	Identyfikator (jeżeli dane są przetwarzane w systemie informatycznym)	Numer i data nadania upoważnienia	Zakres upoważnienia	Data wygaśnięcia/ odwołania upoważnienia	Przyczyna cofnięcia uprawnień
1							

Zał. Nr…..
do instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Zespole Szkół w Rychlikach

Rychliki, dnia ……

UPOWAŻNIENIE NR …….
DO PRZETWARZANIA DANYCH OSOBOWYCH

I.

Upoważniam Panią, Pana ……
(imię i nazwisko)
Zatrudnioną, zatrudnionego w Zespole Szkół w Rychlikach do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku :
……
oraz obsługi systemu informatycznego i urządzeń wchodzących w jego skład .
Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.) i elektronicznej, wg wykazu zbiorów podanych w pkt. II

II.

Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w następujących zbiorach : (proszę wymienić zgodnie z wykazem obowiązujących nazw zbiorów danych osobowych zgodnie z Polityką Bezpieczeństwa Informacji Zespole Szkół w Rychlikach)

1. ……
2. ……
3. ……
4. ……

……
Podpis administratora danych osobowych

OŚWIADCZENIE PRACOWNIKA

III.

Ja niżej podpisana(ny) oświadczam, że :

1. Zostałam(em) przeszkolona(ny) w zakresie ochrony danych osobowych i znana mi jest treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych tj. Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm. oraz „Polityki bezpieczeństwa Informacji w Zespole Szkół w Rychlikach „ i wydanej na jej podstawie instrukcji zarządzania systemem przetwarzania danych osobowych w sposób tradycyjny oraz przy użyciu systemu informatycznego w Zespole Szkół w Rychlikach

2. Zobowiązuję się :

- zachować w tajemnicy dane osobowe, z którymi zetknęłam/ zetknąłem się w trakcie

wykonywana swoich obowiązków służbowych, zarówno w trakcie wykonywania swoich obowiązków służbowych , zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu,
- chronić dane osobowe przed dostępem do nich innych osób do tego nieupoważnionych, zabezpieczać je, przed zniszczeniem i nielegalnym ujawnieniem,
- Znana jest odpowiedzialność karna za naruszenie ww. ustawy (art. 49-54)

…….. ……..

(Podpis administratora danych osobowych) (data i podpis pracownika)

Zał. nr 2

do instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Zespole Szkół w Rychlikach

ODWOŁANIE UPOWAŻNIENIA NR …..
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych odwołuję z dniem ……upoważnienie do przetwarzania danych osobowych wystawione dla Pani/Pana ……..

…… ……
Podpis Administratora Danych (data i podpis pracownika)