

Zarządzenie Nr 1/2013
Dyrektora Zespołu Szkół w Skawie
z dnia 31 stycznia 2013 roku

**w sprawie Instrukcji zarządzania systemem informatycznym służącym do
przetwarzania danych osobowych oraz regulaminy w sprawie ochrony danych
osobowych
w Zespole Szkół w Skawie**

Na podstawie: Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002r. Nr 101, poz. 926, ze zm.) oraz rozporządzenia ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100, poz. 1024).

§1

Dyrektor ustala Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz regulamin w sprawie danych osobowych w Zespole Szkół w Skawie.

§2

Polityka bezpieczeństwa stanowi załącznik 1 do zarządzenia.

§3

Instrukcja stanowi załącznik nr 2 do zarządzenia.

§4

Regulamin stanowi załącznik nr 3 do zarządzenia.

§5

Zarządzenie wchodzi w życie z dniem 1 lutego 2013 roku.

DYREKTOR
ZESPOŁU SZKÓŁ W SKAWIE

mgr inż. Marek Kościelniak

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH

**W
ZESPOLE SZKÓŁ W SKAWIE**

DYREKTOR
ZESPOŁU SZKÓŁ W SKAWIE
M. Kościelniak
mgr inż. Marek Kościelniak

1. WPROWADZENIE	3
2. PODSTAWY PRAWNE.....	3
2.1. Ustawa oraz akty wykonawcze	3
2.2. Definicje.....	4
3. NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH.....	5
3.1. Generalny Inspektor Ochrony Danych Osobowych.....	5
3.2. Przetwarzanie danych	6
3.3. Obowiązki informacyjne o przetwarzaniu danych	7
3.4. Obowiązek zgłoszenia przetwarzania danych.....	8
3.5. Udostępnianie danych	9
3.6. Powierzenie przetwarzania danych	9
3.7. Dokumentowanie	10
3.8. Sankcje karne	10
4. ZAGROŻENIA BEZPIECZEŃSTWA.....	12
4.1. Charakterystyka możliwych zagrożeń	12
4.2. Sytuacje świadczące o naruszeniu zasad bezpieczeństwa	12
4.3. Tabele form naruszenia bezpieczeństwa i sposoby postępowania	13
5. POLITYKA BEZPIECZEŃSTWA.....	16
5.1. Deklaracja	16
5.2. Charakterystyka instytucji.....	16
5.3. Wykaz zbiorów osobowych	16
5.4. Wykaz miejsc przetwarzania.....	17
5.5. Ewidencja osób upoważnionych do przetwarzania danych osobowych	17
5.6. Środki organizacyjne ochrony danych osobowych	17
5.7. Środki techniczne ochrony danych osobowych	19
6. ZAŁĄCZNIKI.....	20

1. WPROWADZENIE

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Zespole Szkół w Skawie z siedzibą 34-713 Skawa 584A zwanym dalej **SZKOŁĄ**.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Do najważniejszych należy ewidencja zbiorów osobowych, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych, a także lista środków organizacyjnych i technicznych służących bezpieczeństwu danych.

2. PODSTAWY PRAWNE

2.1. USTAWA ORAZ AKTY WYKONAWCZE

Przepisy ochrony danych osobowych zawarte są w ustawie o ochronie danych osobowych oraz wydanych do niej aktach wykonawczych. Pełną listę aktów prawnych stanowią:

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926)
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006, Nr 203, poz. 1494) – art. 13.3 ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) – art. 22a ustawy
- 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) – art. 39a ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy.

Niniejszy dokument powstał w oparciu o **art. 36 ust. 2 oraz 39a ustawy o ochronie danych osobowych**, które zobowiązują Administratora danych do wykonania dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych.

Szczegółowy zakres dokumentu określa 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 wydane do art. 39a ustawy.

2.2. DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

Generalny Inspektor Ochrony Danych Osobowych – organ do spraw ochrony danych osobowych.

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Dane wrażliwe - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Administrator danych (ADO) – organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. ADO w szkole jest **Dyrektor**.

Administrator bezpieczeństwa informacji (ABI) – osoba nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Przetwarzanie danych - jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

3. NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

3.1. GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Zadania GODO

Do zadań GODO należy:

- kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach,
- opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

Kontrole GODO

W celu wykonania w/w zadań Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura, zwani dalej „inspektorami”, mają prawo:

- wstępu, w godzinach od 6⁰⁰ do 22⁰⁰, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
- żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
- wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
- przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,
- zlecać sporządzanie ekspertyz i opinii.

Działania GODO w przypadku naruszenie przepisów

W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

- usunięcie uchybień,
- uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
- zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
- wstrzymanie przekazywania danych osobowych do państwa trzeciego,
- zabezpieczenie danych lub przekazanie ich innym podmiotom,
- usunięcie danych osobowych.

W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw **zawiadomienie o popełnieniu przestępstwa**, dołączając dowody dokumentujące podejrzenie.

3.2. PRZETWARZANIE DANYCH

Przetwarzanie danych jest **dopuszczalne** tylko wtedy gdy:

- ☛ Osoba, której dane dotyczą, **wyrazi na to zgodę**, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.
- ☛ Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia **obowiązku wynikającego z przepisu prawa**.
- ☛ Jest to konieczne do **realizacji umowy**, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.
- ☛ Jest niezbędne do **wykonania określonych prawem zadań** realizowanych dla dobra publicznego.
- ☛ Jest to niezbędne dla **wypełnienia prawnie usprawiedliwionych celów** realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Przetwarzanie danych jest **zabronione** w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie tych danych jest **jednak dopuszczalne**, jeżeli:

- ☛ osoba, której dane dotyczą, **wyrazi na to zgodę na piśmie**, chyba że chodzi o usunięcie dotyczących jej danych,
- ☛ **przepis szczególny innej ustawy zezwala** na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
- ☛ przetwarzanie takich danych jest **niezbędne do ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
- ☛ jest to niezbędne do wykonania **statutowych zadań kościołów i innych związków wyznaniowych**, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,
- ☛ przetwarzanie dotyczy danych, które są niezbędne **do dochodzenia praw przed sądem**,

- przetwarzanie jest **niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób**, a zakres przetwarzanych danych jest określony w ustawie,
- przetwarzanie jest prowadzone **w celu ochrony stanu zdrowia**, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
- przetwarzanie dotyczy danych, które zostały podane **do wiadomości publicznej przez osobę**, której dane dotyczą,
- jest to niezbędne do **prowadzenia badań naukowych**, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,
- przetwarzanie danych jest prowadzone przez stronę **w celu realizacji praw i obowiązków wynikających z orzeczenia** wydanego w postępowaniu sądowym lub administracyjnym.

3.3. OBOWIĄZKI INFORMACYJNE O PRZETWARZANIU DANYCH

Zbieranie danych osobowych od osób, których dane dotyczą

W przypadku zbierania danych od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Podanych wyżej zasad **nie stosuje się**, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

Zbieranie danych osobowych nie od osób, których dane dotyczą.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
- źródle danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,
- prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy Administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Podanych wyżej zasad **nie stosuje się**, jeżeli:

- ☛ dane są przetwarzane przez administratora na podstawie przepisów prawa,
- ☛ przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
- ☛ dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

3.4. OBOWIĄZEK ZGŁOSZENIA PRZETWARZANIA DANYCH

Administrator danych jest **obowiązany** zgłosić zbiory danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz zgłaszać zmiany w terminie 30 dni. Zgłoszenie powinno zawierać:

- ☛ wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,
- ☛ oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru,
- ☛ cel przetwarzania danych, w tym opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych,
- ☛ sposób zbierania oraz udostępniania danych, w tym informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,
- ☛ opis środków technicznych i organizacyjnych zastosowanych w celach ochrony danych,
- ☛ informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w dokumentacji ochrony danych osobowych,
- ☛ informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Z obowiązku rejestracji **zwolnieni są** Administratorzy danych:

- ☛ objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,
- ☛ przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym oraz przetwarzanych przez Generalnego Inspektora Informacji Finansowej, a także przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej,
- ☛ dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,
- ☛ przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,
- ☛ dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,
- ☛ tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na Urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego,

- dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych,
- przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

3.5. UDOSTĘPNIANIE DANYCH

Najważniejsze przesłanki i zasady udostępniania danych:

- Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.
- Nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.
- Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
- Dane osobowe, z wyłączeniem danych wrażliwych, mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
- Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
- Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

3.6. POWIERZENIE PRZETWARZANIA DANYCH

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora danych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

- umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron,
- Podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie,
- Podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy oraz spełnić wymagania określone w przepisach, o których mowa w art.39a ustawy. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych,
- odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na Administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Do kontroli zgodności przetwarzania danych przez podmiot, któremu powierzono przetwarzanie danych, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19 ustawy.

3.7. DOKUMENTOWANIE

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do **zagrożeń** oraz **kategorii danych** objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto, Administrator danych:

- prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki organizacyjne i techniczne służące ochronie danych,
- wyznacza **administratora bezpieczeństwa informacji**, nadzorującego przestrzeganie zasad ochrony, chyba, że sam wykonuje te czynności,
- nadaje **upoważnienia do przetwarzania danych** i dopuszcza do pracy wyłącznie osoby posiadające takie upoważnienie,
- **zapewnia kontrolę** nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
- prowadzi **ewidencję osób upoważnionych do ich przetwarzania**, która zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze **rozporządzenia**, sposób prowadzenia i zakres dokumentacji opisującej ochronę danych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

3.8. SANKCJE KARNE

- Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie **nie jest dopuszczalne** albo do których przetwarzania **nie jest uprawniony**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat 2**. Jeżeli czyn ten dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat 3**.
- Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe **niezgodnie z celem utworzenia zbioru**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych **udostępnia je lub umożliwia dostęp** do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **lat 2**. Jeżeli sprawca działa **nieumyślnie**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- Kto administrując danymi **narusza choćby nieumyślnie obowiązek zabezpieczenia** ich przed zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.

- ☛ Kto będąc do tego obowiązany **nie zgłasza do rejestracji zbioru danych**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- ☛ Kto administrując zbiorem danych **nie dopełnia obowiązku poinformowania osoby, której dane dotyczą**, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do **roku**.
- ☛ Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonych w niniejszej dokumentacji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, **wszczyna się postępowanie dyscyplinarne**.
- ☛ Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie **obowiązków pracowniczych**.
- ☛ Orzeczona kara dyscyplinarna **nie wyklucza odpowiedzialności karnej** osoby winnej zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, póź. 926) oraz możliwości wniesienia wobec niej sprawy z **powództwa cywilnego** przez pracodawcę o zrekompensowanie poniesionych strat.

4. ZAGROZENIA BEZPIECZEŃSTWA

4.1. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

- **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona lecz nie dochodzi do naruszenia poufności danych.
- **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych,
- **zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

4.2. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

- **Przełamane zabezpieczenia tradycyjnych** – zerwane plomby na drzwiach, szafach, segregatorach,
- **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych** na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- **jakość danych w systemie** lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- **naruszenie lub próba naruszenia integralności** systemu lub bazy danych w tym systemie,
- **próba lub modyfikacja danych** oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- **niedopuszczalna manipulacja danymi osobowymi** w systemie,
- **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu,
- **praca w systemie lub jego sieci komputerowej** wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
- **ujawnienie istnienia nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki”, itp.,

- **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych,
- **rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

4.3. TABELE FORM NARUSZENIA BEZPIECZEŃSTWA I SPOSOBY POSTĘPOWANIA

Tabela form naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić administratora bezpieczeństwa informacji.
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiegokolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport.
Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.

W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie. Powiadomić przełożonych. Sporządzić raport.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiegokolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakiegokolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakiegokolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość.

informatycznych i telekomunikacyjnych.	Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
--	--

Tabela zjawisk świadczących o możliwości naruszenia ochrony danych osobowych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie administratora bezpieczeństwa informacji oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	
Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie administratora bezpieczeństwa informacji. Sporządzić raport.
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	

Tabela naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	

5. POLITYKA BEZPIECZEŃSTWA

Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

5.1. DEKLARACJA

Administrator danych mając świadomość, iż przetwarza dane **wrażliwe** uczniów deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

5.2. CHARAKTERYSTYKA INSTYTUCJI

Szkoła realizuje zadania głównie na mocy przepisów prawa zawartych w ustawie o systemie oświaty, systemie informacji oświatowej oraz Karcie Nauczyciela, a także innych aktach wykonawczych uprawniających **Dyrektora szkoły** do podejmowania stosownych działań, w tym do przetwarzania danych osobowych. Podstawowym obszarem działania są zadania związane z bezpłatnym nauczaniem.

5.3. WYKAZ ZBIORÓW OSOBOWYCH

Na podstawie § 4 pkt 2 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 **tworzy się wykaz zbiorów osobowych wraz ze wskazaniem programów komputerowych** służących do ich przetwarzania zgodnie z **załącznikiem nr 1** do niniejszej dokumentacji.

Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się, zgodnie z § 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. środki bezpieczeństwa na poziomie **WYSOKIM**.

5.4. WYKAZ MIEJSC PRZETWARZANIA

Na podstawie § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych.

Wyznaczają go pomieszczenia zlokalizowane w Szkole. Szczegółowy wykaz pomieszczeń, stanowi **załącznik nr 2** do niniejszej dokumentacji.

5.5. EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi **załącznik nr 3** do niniejszej dokumentacji.

Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres, a w przypadku kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępu do tego programu.

Ewidencja stanowi podstawę wydania Upoważnienia do przetwarzania danych osobowych na mocy art. 37 ustawy o ochronie danych osobowych.

5.6. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- Przetwarzanie danych osobowych w Szkole może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Zgodnie z art. 36 ust. 3 ustawy o ochronie danych osobowych, Administrator danych **powołuje Administratora bezpieczeństwa informacji**.
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie**. Wzór upoważnienia stanowi **załącznik nr 4** do niniejszej dokumentacji.
- ABI prowadzi **ewidencję osób upoważnionych**, o której mowa w pkt 5.5 oraz na jej podstawie przygotowuje **Upoważnienia do przetwarzania danych** i przedkłada je do podpisu ADO.
- Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego **załącznik nr 5** do niniejszej dokumentacji.
- Zabrania się przetwarzania danych poza obszarem określonym w załączniku nr 2 do niniejszej dokumentacji.
- Każdy pracownik Szkoły co najmniej raz na 2 lata musi odbyć **szkolenie z zakresu ochrony danych osobowych**. Za organizację szkoleń odpowiedzialny jest ABI, który prowadzi w tym celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
- Ponadto każdy upoważniony do przetwarzania danych **potwierdza pisemnie** fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi **załącznik nr 6** do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych.

- Obszar przetwarzania danych osobowych określony w załączniku nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
- Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio **załącznik nr 7** oraz **załącznik nr 8** do przedmiotowej dokumentacji.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w **załączniku nr 10**.

Dla zapewnienia kontroli przestrzegania zasad określonych w niniejszej dokumentacji wyznacza się następujące **zadania Administratorowi bezpieczeństwa informacji**:

- Nadzór nad przetwarzaniem danych zgodnie z ustawą o ochronie danych osobowych i innymi przepisami prawa.
- Kontrola przestrzegania zasad ochrony – systematycznie, nie rzadziej niż dwa razy do roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:
 - Kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony.
 - Kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są informacje.
 - Kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi.
 - Kontrola awaryjnego zasilania komputerów.
 - Nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych.
 - Kontrola systemu kontroli obecności wirusów komputerowych.
 - Kontrola wykonywania kopii awaryjnych.
 - Kontrola przeglądu, konserwacji oraz uaktualnienia systemów informatycznych.
 - Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.
 - Kontrola nadanych upoważnień.
- Przedstawianie Administratorowi danych wyników kontroli.
- Systematyczna analiza dokumentacji pod kątem obszarów, zbiorów oraz zasad ochrony.
- Szkolenie z ochrony danych osobowych oraz aktów wykonawczych.
- Podjęcie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu bezpieczeństwa informacji.

- Prowadzenie monitoringu przetwarzania danych.
- Każdorazowe sporządzenie raportu zgodnie ze wzorem będącym **załącznikiem nr 9** do niniejszej dokumentacji oraz przedstawienie efektów działań Administratorowi danych.

5.7. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

Zbiory danych przetwarzane w Szkole zabezpiecza się poprzez:

1. Środki ochrony fizycznej.

- Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie.
- Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą , rolet.
- Pomieszczenia, w którym przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
- Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie.
- Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
- Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.

- Zbiory danych osobowych przetwarzane są przy użyciu komputera stacjonarnego i przenośnego .
- Komputer służący do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową.
- Zastosowano urządzenia typu UPS, i wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
- Użyto system Firewall do ochrony dostępu do sieci komputerowej.

3. Środki ochrony w ramach systemowych narzędzi programowych i baz danych.

- Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
- Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych .

E. ZAŁĄCZNIKI

Załącznik nr 1. Wykaz zbiorów osobowych przetwarzanych w Szkole.

Załącznik nr 2. Wykaz miejsc przetwarzania zbiorów osobowych w Szkole.

Załącznik nr 3. Wykaz osób upoważnionych do przetwarzania danych osobowych w Szkole.

Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.

Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

Załącznik nr 7. Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych.

Załącznik nr 8. Wzór odwołania zgody na przebywanie w obszarze przetwarzania danych osobowych.

Załącznik nr 9. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.

Załącznik nr 10. Wzór zgody na przetwarzanie danych.

WYKAZ ZBIORÓW OSOBOWYCH

Lp.	Nazwa zbioru - opis DOKUMENTACJA SŁUŻĄCA DO PRZETWARZANIA ZBIORU DANYCH Nazwa zbioru - opis	Struktura zbioru	Systemy informatyczne	MIEJSCE PRZETWARZANIA /ODPOWIEDZIALNY/	Zastosowany Poziom bezpieczeństwa	Zgłoszenie GIODO
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						

WYKAZ MIEJSC PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa pomieszczenia	Adres
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		

**EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH
OSOBOWYCH**

Lp.	Nazwisko, Imię	Nr zbiorów	Okres upoważnienia		Program/identyfikator	Uwagi
			OD	DO		
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
11						
12						

Skawa, dn. ____ - ____ - ____ r.

WAŻNOŚĆ

od:

do: *do odwołania*

UPOWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101 poz. 926, ze zm.) upoważniam Panią/Pana:

.....

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

Nr zbiorów z ewidencji zbiorów	Nazwa programu / identyfikator

.....
(podpis Administratora danych)

Skawa , dn. __ - __ - ____ .

UNIEWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101 poz. 926, ze zm.) unieważniam upoważnienie do przetwarzania danych osobowych wydane dniadla Pani/Pana:

.....

.....
(podpis Administratora danych)

Skawa, dn. __ - __ - ____ r.

.....
(imię i nazwisko pracownika)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść:

- a) dokumentacji ochrony danych osobowych w Zespole Szkół w Skawie,
- b) Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926),
- c) 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).

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy, a w szczególności nie będę:

- a) ujawniać danych zawartych w eksploatowanych w systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
- b) ujawniać szczegółów technologicznych używanych w systemów oraz oprogramowania,
- c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
- d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą Dokumentacją.

.....
(podpis pracownika)

.....
(podpis Dyrektora)

Skawa, dn. __ - __ - ____ r.

WAŻNOŚĆ

od:

do:

ZGODA
NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.), **wyrażam zgodę Pani/Panu:**

.....

na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych.

.....
(podpis Administratora danych)

Skawa, dn. __ - __ - ____ r.

ODWOŁANIE ZGODY NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.), **odwołuję zgodę** z dnia o sygnaturze udzieloną **Pani/Panu:**

.....

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe.

.....
(podpis Administratora danych)

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w Zespole Szkół w Skawie

1. Data: Godzina:
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:

.....
.....
.....

6. Podjęte działania:

.....
.....
.....

7. Postępowanie wyjaśniające:

.....
.....
.....

.....
(data, podpis Administrator danych)

Skawa, dn. ____ - ____ - ____ r.

.....
(imię i nazwisko, adres zamieszkania)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Na podstawie art. 23 ust.1 pkt 1 (oraz/lub art. 27.2 pkt 1 – dla danych wrażliwych) ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926), wyrażam zgodę na przetwarzanie niżej wymienionych moich danych osobowych.

Zgoda udzielona jest tylko do przetwarzania danych oraz ich udostępniania w podanym niżej zakresie.

Lp.	Zakres danych – zgoda	Cel przetwarzania	Odbiorcy lub kategorie odbiorców danych
1			
2			
...			

Jednocześnie zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926) przyjmuję do wiadomości, że:

- Administratorem danych jest Zespół Szkół w Skawie z siedzibą 34-713 Skawa 584a,
- dane będą przetwarzane wyłącznie zgodnie z określonym celem,
- dane będą udostępniane wyłącznie podanym odbiorcom,
- przysługuje mi prawo dostępu do treści danych oraz ich poprawiania,
- dane podaję dobrowolnie.

.....
(podpis)

WYKAZ ZBIORÓW OSOBOWYCH

Lp.	Nazwa zbioru - opis DOKUMENTACJA SŁUŻĄCA DO PRZETWARZANIA ZBIORU DANYCH	Struktura zbioru	Systemy informatyczne	Miejsce przetwarzania /odpowiedzialny/	Zastosowany Poziom Bezpieczeństwa	Zgłoszenie GIODO
ZBIÓR DANYCH OSOBOWYCH - UCZNIOWIE						
1.	Księga Ewidencji Dzieci w Placówce - coroczna adnotacja o spełnianiu przez dziecko obowiązku szkolnego w tej albo innej szkole	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		Sekretariat Sekretarka	Wysoki	TAK
2.	Karta zapisu dziecka do szkoły - Informacje dot. ucznia przyjmowanego do szkoły	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, wizerunek dziecka, telefon, przynależność wyznaniowa		Sekretariat Gabinet dyrektora Dyrektor Sekretarka	Wysoki	NIE (art. 43.1. pkt. 4)
3.	Księga Uczniów - Zbiór danych o uczniach	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu,		Sekretariat Sekretarka	Wysoki	TAK

		pesel zawód, przyjęcie do szkoły: data, klasa semestr, obwód szkolny. Wypisanie ze szkoły: data, klasa, powody, Data: wydania dok, ukończenia szkoły numer wydanego świadectwa				
4.	Dziennik Lekcyjny - Dokumentacja przebiegu nauczania w danym roku szkolnym	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu,	LIBRUS	Sale lekcyjne Nauczyciele Wychowawcy	Wysoki	NIE (art. 43.1. pkt 4)
5.	Arkusz Oceny - dokumentacja wyników nauczania ucznia w poszczególnych latach	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, nr księgi uczniów, przebieg nauki, wyniki nauki	LIBRUS	Gabinet dyrektora Dyrektor Wychowawcy Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
6.	Ewidencja świadectw szkolnych	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel		Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)
7.	Arkusz dostosowania wymagań	Nazwisko, imię dziecka, imiona rodziców, data urodzenia miejsce urodzenia, numer opinii lub orzeczenia informacje dot. rozwoju dziecka, formy dostosowania wymagań		Dyrektor Wychowawcy Nauczyciele Pedagog	Wysoki	NIE (art. 43.1. pkt 4)

8.	Ewidencja legitymacji szkolnych	Nazwiska, imiona, pesel		Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
9.	Ewidencja kart rowerowych	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania		Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
10.	Protokoły Rady Pedagogicznej - Protokoły z posiedzenia Rady Pedagogicznej	Nazwiska i imiona, stan zdrowia,		Gabinet dyrektora Protokolant Rada Pedagogiczna Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)
11.	Okręgowa Komisja Egzaminacyjna	Nazwisko, imiona, data i miejsce urodzenia, Pesel, płeć, dysleksja, mniejszość narod.	OKE, CKE	Gabinet dyrektora Dyrektor Biblioteka nauczyciel bibliotekarz	Wysoki	NIE (art. 43.1. pkt 4)
12.	Stypendia	Imię, nazwisko, data urodzenia, adres zamieszkania,		ZEAS RABA W. Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
13.	Wyprawa szkolna	Nazwisko, imię ucznia, data urodzenia, miejsce urodzenia, adres zamieszkania, imiona i nazwiska rodziców, adres zamieszkania, PESEL rodzica, dziecka, dochód		ZEAS Raba Wyżna Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)

14.	Biblioteka	Nazwisko, imię, adres zam., dane o wypożyczeniach	LIBRUS, MOL KSEON	Biblioteka Bibliotekarz	Wysoki	NIE (art. 43.1. pkt 4)
15.	Dziennik Pedagoga szkolnego - Dziennik zawiera informacje o dzieciach zakwalifikowanych do różnych form pomocy	Nazwiska i imiona, Informacje o kontaktach z innymi osobami, instytucjami, stan zdrowia	LIBRUS	Pedagog	Wysoki	NIE (art. 43.1. pkt 4)
16.	Dokumentacja Pedagoga - Dokumentacja badań i czynności uzupełniających prowadzonych przez pedagoga	Różne dane niezbędne do dokumentowania przebiegu terapii, nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia, opinia PPP		Koordynator do spraw pomocy pedagogiczno-psychologicznej	Wysoki	NIE (art. 43.1. pkt 4)
17.	Dokumentacja pielęgniarstwa szkolnej	Nazwiska i imiona, Informacje o kontaktach z innymi osobami, instytucjami, stan zdrowia		Pielęgniarka	Wysoki	NIE (art. 43.1. pkt 4)
18.	Lista uczestników wycieczek	Nazwisko i imię, wiek, data urodzenia, adres zamieszkania, PESEL	LIBRUS	Sekretariat Sekretarka Gabinet dyrektora Dyrektor	Wysoki	TAK
19.	Ubezpieczenie uczniów	Imiona nazwiska, adres zamieszkania lub pobytu		Sekretariat Sekretarka Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)

20.	Dokumentacja wypadków uczniów - informacje o wypadkach uczniów	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia		Gabinet dyrektora Dyrektor Sekretariat Sekretarka Koordynator ds. bezpieczeństwa	Wysoki NIE (art. 43.1. pkt 4)	
21.	Opinie i Orzeczenia Poradni Psychologiczno-Pedagogicznej	Imię i nazwisko, data urodzenia, stan zdrowia	LIBRUS	Dyrektor Nauczyciele	Wysoki NIE (art. 43.1. pkt 4)	
22.	Dziennik zajęć pozalekcyjnych	Imię i nazwisko, data urodzenia adres zamieszkania, imiona i nazwisko rodziców,	LIBRUS	Sale lekcyjne Nauczyciele	Wysoki NIE (art. 43.1. pkt 4)	
23.	Dziennik indywidualnego nauczania	Imię i nazwisko, data urodzenia adres zamieszkania, imiona i nazwisko rodziców,	LIBRUS	Sala lekcyjna Nauczyciel nauczania indywidualnego	Wysoki NIE (art. 43.1. pkt 4)	
24.	Dziennik zajęć z art. 42KN	Imię i nazwisko, data urodzenia adres zamieszkania, imiona i nazwisko rodziców,	LIBRUS	Sale lekcyjne Nauczyciele	Wysoki NIE (art. 43.1. pkt 4)	
25.	Dziennik bibliotekarza	Imię i nazwisko, data urodzenia adres zamieszkania, imiona i nazwisko rodziców,	LIBRUS	Biblioteka Bibliotekarz	Wysoki NIE (art. 43.1. pkt 4)	

26.	Zgody na przetwarzanie danych	Imię i nazwisko adres udzielającego zgodę	Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)
-----	-------------------------------	---	----------------------------	--------	---------------------------

ZBIÓR DANYCH OSOBOWYCH - PRACOWNICY

27.	Akta osobowe - Zbiór zatrudnionych pracowników	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, nr dowodu osobistego, wykształcenie, przebieg dotychczasowego zatrudnienia, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia	LIBRUS	Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
28.	Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych	Nazwisko, imię, stanowisko, login, podpis		Gabinet dyrektora Dyrektor-ADO ABI	Wysoki	NIE (art. 43.1. pkt 4)
29.	Dokumentacja nadzoru pedagogicznego	Nazwiska i imiona, zajmowane stanowisko		Gabinet dyrektora Dyrektor	Wysoki	
30.	Dokumentacja dotycząca polityki kadrowej-opiniowanie awansów, wyróżnień, odznaczeń, nagród, itp.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, wykształcenie,		Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)

31.	Ewidencja zwolnień lekarskich pracowników	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania /nieobecności w pracy?	Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
32.	Orzeczenia lekarskie do celów sanitarno-epidemiologicznych	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania , stanowisko	Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)
33.	Ewidencja urlopów pracowniczych	Nazwiska i imiona, adres zamieszkania	Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)
34.	Karty czasu pracy	Nazwiska i imiona, adres zamieszkania	Sekretariat Sekretarka Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)
35.	Listy płac pracowników	Nazwiska i imiona, adres zamieszkania	Archiwum Dyrektor Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
36.	Rejestr delegacji służbowych	Nazwiska i imiona, adres zamieszkania	Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
37.	Rejestr wydanej odzieży i środków ochrony indywidualnej	Nazwiska i imiona, adres zamieszkania	Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)

38.	System Informacji Oświatowej Zbiór zawiera informacje o nauczycielach i uczniach szkoły	PESEL, miejsce pracy, zawód, wykształcenie, wynagrodzenie	SIO	Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)
39.	Świadczenia socjalne dla pracowników	Nazwiska i imiona, adres zamieszkania lub pobytu, stan zdrowia, dochody brutto		Gabinet dyrektora Dyrektor Członkowie Komisji ZFŚS Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
40.	Dobrowolne ubezpieczenie pracowników	Imiona nazwiska, adres zamieszkania lub pobytu, PESEL, nr telefonu		Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
41.	Dokumentacja wypadków pracowników - Informacje o wypadkach pracowników	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, stan zdrowia		Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
42.	Umowy zlecenia	Nazwiska i imiona, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu		Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)

43.	Przelewy	Nazwiska, imiona, adresy zamieszkania, nr kont bankowych kontrahentów będących osobami fizycznymi, NIP, wyciągi bankowe		Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4) (warunkowo)
44.	Klienci	Nazwisko, imię, adres, nr dowodu osobistego		Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	TAK
45.	Faktury	Nazwisko, imię, adres zamieszkania	RACHUNEK	Gabinet dyrektora Dyrektor ZEAS RABA W Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 8)
46.	Książka korespondencyjna	Imię i nazwisko, adres zamieszkania		Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	TAK
47.	Ubezpieczenie ZUS - Informacje o pracownikach potrzebne do ubezpieczenia w ZUS	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, PESEL, NIP	Płatnik	Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)
48.	Awans Zawodowy Teczki awansu zawodowego	Imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zam. przebieg		Gabinet dyrektora Dyrektor	Wysoki	NIE (art. 43.1. pkt 4)

		zatrudnienia, wykształcenie, składniki wynagrodzenia, zapytanie o karalność, stan zdrowia,				
49.	Kandydaci na pracowników	Imię, nazwisko, data i miejsce urodzenia, adres zamieszkania, telefon, kwalifikacje	Gabinet dyrektora Dyrektor Sekretariat Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)	
50.	Dokumenty archiwalne	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 nr księgi uczniów, przebieg nauki, wyniki nauki 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	Archiwum Dyrektor Sekretarka	Wysoki	NIE (art. 43.1. pkt 4)	

ZESPÓŁ SZKÓŁ W SKAWIE
34-713 Skawa 584 A
tel./fax 018 26 86 722
NIP 7352746966, REGON 120747074

ZBIORY DANYCH PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	MIEJSCE PRZETWARZANIA	ODPOWIEDZIALNY
Pracownicy	SIO	gabinet dyrektora szkoły sekretariat	DYREKTOR WICEDYREKTOR SEKRETARKA
	e-Świadectwa	gabinet dyrektora szkoły/pracownia informatyczna	WYCHOWAWCY mgr PIOTR STOPKA
	OKE	gabinet dyrektora szkoły sekretariat	DYREKTOR/ WICEDYREKTOR SEKRETARKA
	CKE	gabinet dyrektora szkoły/ biblioteka/sekretariat	DYREKTOR/ WICEDYREKTOR NAUCZYCIEL BIBLIOTEKARZ /SEKRETAKKA
	OBUT	gabinet dyrektora szkoły	DYREKTOR/WYCHOWAWCA / WICEDYREKTOR
	OPERON	gabinet dyrektora szkoły	DYREKTOR/WYCHOWAWCA / WICEDYREKTOR
	BIP	gabinet dyrektora szkoły pracownia informatyczna	DYREKTOR mgr PIOTR STOPKA
	GIS	gabinet dyrektora szkoły	DYREKTOR
	LIBRUS	Pomieszczenia edukacyjne szkoły Sekretariat, gabinet dyrektora szkoły	DYREKTOR/ WICEDYREKTOR NAUCZYCIEL BIBLIOTEKARZ /SEKRETAKKA/NAUCZYCIELE
Rachunek KSEON		gabinet dyrektora szkoły	DYREKTOR/ WICEDYREKTOR
		Biblioteka	NAUCZYCIEL BIBLIOTEKARZ

DYREKTOR
ZESPÓŁU SZKÓŁ W SKAWIE

mgr inż. Marek Kościelniak

Załącznik Nr 2
do Zarządzenia Nr 1/2013
Dyrektora Zespołu Szkół w Skawie
z dnia 31 stycznia 2013r.

ZESPÓŁ SZKÓŁ W SKAWIE
34-713 Skawa 584 A
tel./fax 018 26 86 722
NIP 73352746966, REGON 120747074

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMACYJNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ W SKAWIE

Administrator Danych osobowych

DYREKTOR
ZESPOŁU SZKÓŁ W SKAWIE
mgr inż. Marek Kościelnik

SPIS TREŚCI

1. Postanowienia ogólne.....	3
2. Przeznaczenie, definicje	3
3. Określenie bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.....	5
4. Zasady prowadzenia ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych	5
5. Charakterystyka systemu	6
6. Ogólne zasady pracy w systemie informatycznym	6
7. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności	7
8. Stosowanie metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem	7
9. Procedury tworzenia kopii awaryjnych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania	8
10. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.....	9
11. Sposób zabezpieczenia systemu przed działanością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.....	10
12. Informacje o odbiorcach, które dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia	10
13. Przesyłanie danych poza obszar przetwarzania	11
14. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników służących do przetwarzania danych	11
15. Postanowienia końcowe	12

I. POSTANOWIENIA OGÓLNE

Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. 2002r. Nr 101, poz. 926, ze zm.) oraz rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100, poz. 1024) nakłada na administratora danych osobowych następujące obowiązki:

- zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
- zabezpieczenie danych przed nieuprawnionym dostępem,
- zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
- zabezpieczenie przed utratą danych,
- zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.

Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i system informatyczny, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

II. PRZEZNACZENIE, DEFINICJE

Instrukcja zarządzania systemie informatycznym, służącym do przetwarzania danych osobowych w **ZESPOLU SZKÓŁ W SKAWIE**, zwaną dalej instrukcją - określa sposób zarządzania oraz zasady administrowania systemem informatycznym służącym do przetwarzania danych osobowych.

Ilkroć w instrukcji jest mowa o:

1. **Jednostce** - rozumie się przez to **ZESPÓŁ SZKÓŁ W SKAWIE**;
2. **Kierownictwie** - rozumie się przez to **Dyrektora Jednostki**;
3. **Danych osobowych** - rozumie się przez to każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby;
4. **Zbiórze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie;

5. **Przetwarzaniu danych** - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonywane są w systemach informatycznych;

6. **Usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

7. **Administratorze bezpieczeństwa informacji (ABI)** - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w wypadku naruszeń w systemie zabezpieczeń;

8. **Administratorze sieci/systemu operacyjnego** - rozumie się przez to osobę nadzorującą i odpowiadającą za poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego w danej jednostce organizacyjnej, w tym w szczególności:

- mającą prawo do zmiany uprawnień wszystkich użytkowników,
- za pomocą platformy zarządzania dysponującą bezpośrednio wszystkimi zasobami podległej mu sieci,
- pełniącą kontrolę nad dostępem użytkowników do systemów,
- podejmującą samodzielnie lub na polecenie administratora bezpieczeństwa informacji odpowiednie działania w wypadku naruszeń w systemie zabezpieczeń.

9. **Administratorze aplikacji** - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo przetwarzania danych w ramach aplikacji, w tym administrującą prawami dostępu w ramach ekspluatowanych aplikacji;

10. **Użytkownikach systemu** - rozumie się osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym;

11. **Obszarze kontrolowanym** - należy przez to rozumieć obszar znajdujący się pod ochroną, o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych, w tym danych osobowych.

Niniejsza Instrukcja zarządzania systemem informatycznym określa:

a) określenie poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym;

b) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym;

c) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem;

d) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności;

- e) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
- f) metoda i częstotliwość tworzenia kopii awaryjnych.
- g) metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania;
- h) sposób, miejsce i okres przechowywania:
- elektronicznych nośników informacji zawierających dane osobowe;
 - kopii zapasowych;
- i) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
- j) sposób postępowania w zakresie komunikacji w sieci komputerowej;
- k) procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

III. OKREŚLENIE POZIOMU BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMACYJNYM

1. Z analizy zagrożeń wynika, że w jednostce miejscami najbardziej zagrożonymi są pomieszczenia budynku, w których znajdują się zbiory danych osobowych gromadzone w kartotekach oraz urządzeniach służących do przetwarzania tych danych, do których mogą mieć nieuprawniony dostęp osoby nieupoważnione spoza jednostki.
2. W systemie informatycznym jednostki przetwarzane są dane osobowe UCZNIÓW I RODZICÓW, DANE OSOBOWE NAUCZYCIELI I POZOSTAŁYCH PRACOWNIKÓW SZKOŁY.

IV. ZASADY PROWADZENIA EWIDENCJI PRACOWNIKÓW ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Administrator bezpieczeństwa informacji prowadzi ewidencję wszystkich pracowników jednostki zatrudnionych przy przetwarzaniu danych osobowych.
2. Powyższa ewidencja uwzględnia:

- dane personalne pracownika (imię i nazwisko),
- zakres uprawnień (nr zbioru),
- okres upoważnienia,
- program/identyfikator,
- stanowisko,
- podpis.

3. Jakakolwiek zmiana informacji wyszczególnionej w ewidencji podlega natychmiastowemu odnotowaniu.

V. CHARAKTERYSTYKA SYSTEMU

1. Sieć informatyczna ma strukturę gwiazdy ze switchem centralnym, do którego podłączony jest serwer oraz komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie.

VI. OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. ABI odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjnych-funkcjonalnych.
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ABI do eksploatacji licencjonowane oprogramowanie.
3. ABI prowadzi ewidencję oprogramowania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

- a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
- b. mechanizmy umożliwiające wykonywanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
- c. urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
- d. mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
- e. mechanizmy zarządzania zmianami.

5. Użytkownikom zabrania się:

- a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy Szkoły bez pisemnej zgody ADO,
- b. udostępniania stanowisk roboczych osobom nieuprawnionym,
- c. wykorzystywania sieci komputerowej Szkoły w celach innych niż wyznaczone przez ADO,
- d. samowolnego instalowania i używania programów komputerowych,
- e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,

- f. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej Szkoły oraz sieci Internetowej osobom nieuprawnionym,
- g. używania komputera bez zainstalowanego oprogramowania antywirusowego.

VII. PROCEDURY NADAWANIA UPRAWNIEN DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEN W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Użytkowników systemu informatycznego tworzy oraz usuwa ABL na podstawie zgody ADO.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi załącznik nr 3 do Polityki bezpieczeństwa przetwarzania danych.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
 - a. nieobecności pracownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
 - b. zawieszenia w pełnieniu obowiązków służbowych.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

VIII. STOSOWANIE METODY I ŚRODKI WIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniejszego zarejestrowanego użytkownika ABL, nadaje inny identyfikator odstępując od ogólnej zasady.
4. W identyfikatorze pomija się polskie znaki diakrytyczne.
5. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką.
6. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.

7. Hasła użytkowników generuje ABI i przekazuje wraz z loginem w formie papierowej w zamkniętej kopercie.
8. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.
9. Hasło nie może być zapisywane i przechowywane.
10. Użytkownik nie może udostępniać identyfikatora oraz hasła osobom nieupoważnionym.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY.

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.
3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.
5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.
6. ABI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

IX. PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
4. Za proces tworzenia kopii awaryjnych na serwerze odpowiada ABI.

5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu informatycznego zobowiązani są do wykonywania samodzielnie kopii bezpieczeństwa tych zbiorów.

6. Kopie awaryjne mogą być wykonywane tylko na nośnikach informatycznych dostarczonych przez ABI.

7. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.

8. Kopie awaryjne wykonuje się po znaczących zmianach w wprowadzonych danych w programie.

9. Kopie awaryjne przechowuje ABI, a w przypadku przetwarzania danych na stacjach roboczych poszczególne użytkownicy. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.

10. ABI zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.

11. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.

X. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ABI w odpowiednio zabezpieczonym pomieszczeniu.

2. Dane osobowe gromadzone są na stacjach roboczych oraz na nośnikach zewnętrznych. Przenośne nośniki danych zabezpieczone są hasłem.

4. 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 odczytanie,

c. **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ABI.

5. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez ABI.

XI. SPOŚB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. ABI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:

- a. skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera,
- b. skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.
- c. automatycznej aktualizacji wzorców wirusów.

2. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ABI.

3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ABI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

- a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- b. odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
5. ABI monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

XII. INFORMACJE O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA

1. Informacje o udostępnieniu danych osobowych przetwarzają się i przechowują w oparciu o Rzeczkowy Wykaz Akt i Instrukcję kancelaryjną.
2. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.
3. Nadzór nad właściwym udostępnianiem danych prowadzi ABI.

XIII. PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez hasło dostępu.
2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
 - a. zatwierdzenie przez ABI zakresu danych osobowych przeznaczonych do wysłania,
 - b. zastosowanie mechanizmów szyfrowania danych osobowych,
 - c. zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisję danych osobowych oraz rejestrację transmisji wysyłania danych osobowych.
3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

XIV. PROCEDURY WYKONYWANIA PRZEGŁĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymagane poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ABI.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ABI.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Szkołą, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. ABI wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

XIV. POSTANOWIENIA KOŃCOWE

1. Każda osoba wpisana do ewidencji zobowiązana jest do odbycia stosownego przeszkolenia w zakresie ochrony danych osobowych oraz zapoznania się z:
 - treścią ustawy oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
 - polityką bezpieczeństwa - regulaminem ochrony danych osobowych;
 - instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
 - uregulowaniami wewnętrznymi obowiązującymi w tym zakresie.
2. Wykonanie powyższych zobowiązań pracownik potwierdza własnoręcznym podpisem.
3. Wszelkie zagadnienia dotyczące ochrony danych osobowych nie ujęte w niniejszej „Instrukcji” należy rozpatrywać zgodnie z treścią aktów prawnych wymienionych w regulaminie ochrony danych osobowych”, z uwzględnieniem późniejszych zmian i uzupełnień.
4. Instrukcja niniejsza wchodzi w życie z dniem zatwierdzenia jej przez Dyrektora Jednostki (administratora danych osobowych).

Załącznik Nr 3

do Zarządzenia Nr 1/2013

Dyrektora Zespołu Szkół w Skawie

z dnia 31 stycznia 2013r.

ZESPÓŁ SZKÓŁ W SKAWIE
34-713 Skawa 584 A
tel./fax 018 26 86 722
NIP 7352746966, REGON 120747074

REGULAMIN W SPRAWIE OCHRONY DANYCH OSOBOWYCH OBOWIĄZUJĄCY W ZESPOLE SZKÓŁ W SKAWIE

W celu zapewnienia ochrony przetwarzanych danych osobowych administrator danych osobowych, Zespół Szkół w Skawie, na podstawie art. 36 w związku z art. 3 i 7 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) wprowadza poniższy REGULAMIN.

DYREKTOR
ZESPÓŁ SZKÓŁ W SKAWIE
mgr inż. Marek Kościelnik

SPIS TREŚCI

1. Przeznaczenie, definicje	3
2. Przepisy ogólne	5
3. Udostępnianie danych ze zbioru	6
4. Gromadzenie i przetwarzanie danych osobowych	8
5. Szczegółne zasady bezpieczeństwa	11
6. Odpowiedzialność za naruszenie instrukcji	13
7. Zmiany instrukcji	14
8. Moc obowiązująca	14

I. Przeznaczenie, definicje

§ 1

Regulamin niniejszy określa tryb i zasady ochrony danych osobowych przetwarzanych w Zespole Szkół w Skawie zwanym dalej Jednostką.

1. Ilekroć w regulaminie jest mowa o:

- a) **Jednostce** – rozumie się przez to **Zespół Szkół w Skawie**.
- b) **zbiore danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- c) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- d) **przetwarzaniu danych** - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- e) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych osobowych;
- f) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
- g) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
- h) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- i) **administratorze danych osobowych** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Dyrektora Jednostki, który decyduje o celach danych osobowych przetwarzania danych osobowych;
- j) **administratorze bezpieczeństwa informacji**- rozumie się przez to osobę wyznaczoną przez Dyrektora Jednostki, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

k) **administratorze systemu informatycznego** - rozumie się przez to osobę zatrudnioną przez Dyrektora Jednostki, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

l) **użytkowniku systemu informatycznego** - rozumie się przez to upoważnionego przez Dyrektora Jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;

m) **zgodzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

II. Przepisy ogólne

§ 2

1. Przetwarzanie danych osobowych do celów związanych z działalnością administratora danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów administratora danych powinna być dokonywana indywidualnie w każdej sytuacji - w razie wątpliwości należy kontaktować się z reprezentantem.

§ 3

1. Administrator danych gromadzi i przetwarza dane osobowe w następujących celach:

a) wykonywanie obowiązków pracodawcy w zakresie zatrudnienia pracowników (dokumentacja i przebieg zatrudnienia oraz płace pracowników)

b) realizacja zadań statutowych w stosunku do dzieci, ich prawnych opiekunów oraz innych osób korzystających z usług świadczonych przez administratora danych, w zakresie wykonywanych zadań.

2. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:
- a) adresie swojej siedziby i pełnej nazwie,
 - b) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
 - c) prawie wglądu do swoich danych oraz ich poprawiania,
 - d) dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
3. Powyższy obowiązek administrator danych nakłada na osoby zatrudnione przy gromadzeniu i przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonywania.

§ 4

1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:
- 1) adresie swojej siedziby i pełnej nazwie,
 - 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
 - 3) źródle danych,
 - 4) prawie wglądu do swoich danych oraz ich poprawiania,
 - 5) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych,
 - a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą
 - 6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobom innym administratorowi danych.
2. Powyższy obowiązek administrator danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonywania.

III. Udostępnianie danych ze zbioru

§ 5

1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

- 1) jakie dane osobowe zawiera zbiór
- 2) w jaki sposób zebrano dane
- 3) w jakim celu i zakresie dane są przetwarzane
- 4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 6

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

- 1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
- 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
- 3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania w powszechnie zrozumiałej formie treści tych danych,

4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,

5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji, dla którego zostały zebrane,

7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych,

a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,

8) wniesienie sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów

administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowym innemu administratorowi danych,

9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyjątkowo wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt. 1 - 5, nie częściej niż raz na 6 miesięcy.

§ 7

1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu, do których tryb ich uzupełnienia, aktualizowania lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować reprezentanta.

IV. Gromadzenie i przetwarzanie danych osobowych

§ 8

1. W siedzibie administratora tworzy się następujące zbiory danych osobowych:

w stosunku do dzieci, uczniów oraz ich prawnych opiekunów:

1. Księga Ewidencji Dzieci w Szkole Podstawowej - Coroczna adnotacja o spełnianiu przez dziecko obowiązku szkolnego w tej albo innej szkole.
2. Karta zapisu dziecka do szkoły - Informacje dot. ucznia przyjmowanego do szkoły.
3. Księga Ewidencji Uczniów - Zbiór danych o uczniach.
4. Dziennik Lekcyjny - Dokumentacja przebiegu nauczania w danym roku szkolnym.
5. Arkusz Oceny - dokumentacja wyników nauczania ucznia w poszczególnych latach.

6. Ewidencja świadczeń szkolnych.
 7. Arkusz dostosowania wymagań.
 8. Ewidencja legitymacji szkolnych.
 9. Ewidencja kart rowerowych.
 10. Protokoły Rady Pedagogicznej -Protokoły z posiedzenia Rady Pedagogicznej.
 11. Okręgowa Komisja Egzaminacyjna.
 12. Stypendia.
 13. Wyprawka szkolna.
 14. Biblioteka.
 15. Dziennik Pedagogia/Logopedy szkolnego - Dziennik zawiera informacje o dzieciach zakwalifikowanych do różnych form pomocy.
 16. Dokumentacja Pedagogia/Logopedy - Dokumentacja badań i czynności uzupełniających prowadzonych przez pedagoga/logopedy.
 17. Lista uczestników wycieczek.
 18. Ubezpieczenie uczniów.
 19. Dokumentacja wypadków uczniów - Informacje o wypadkach uczniów.
 20. Opinie i Orzeczenia Poradni Psychologiczno-Pedagogicznej.
 21. Dziennik zajęć pozalekcyjnych.
 22. Dziennik indywidualnego nauczania.
 23. Dziennik zajęć z art.42 KN.
 24. Dziennik bibliotekarza.
 25. Zgody na przetwarzanie danych.
- w stosunku do pracowników, kadry i personelu:**

26. Akta osobowe - Zbiór zatrudnionych pracowników.
27. Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych.
28. Dokumentacja nadzoru pedagogicznego.
29. Dokumentacja dotycząca polityki kadrowej–opiniowanie awansów, wyróżnień, odznaczeń, nagród, wniosków o odznaczenia, itp.
30. Ewidencja zwolnień lekarskich pracowników.
31. Orzeczenia lekarskie do celów sanitarno-epidemiologicznych.
32. Ewidencja urlopów pracowników.
33. Karty czasu pracy.
34. Listy płac pracowników.

35. Rejestr delegacji służbowych.
36. Rejestr wydanej odzieży i środków ochrony indywidualnej.
37. System Informacji Oświatowej Zbiór zawiera informacje o nauczycielach i uczniach szkoły.

38. Świadczenia socjalne dla pracowników.
39. Dobrowolne ubezpieczenie pracowników.
40. Dokumentacja wypadków pracowników - Informacje o wypadkach pracowników.
41. Umowy zlecenia.
42. Przelewy.
43. Klienci.
44. Faktury.

45. Książka korespondencyjna.
46. Ubezpieczenie ZUS - Informacje o pracownikach potrzebne do ubezpieczenia w ZUS.
47. Awans Zawodowy Teczki awansu zawodowego.
48. Kandydaci na pracowników.
49. Dokumenty archiwalne.

2. Dane osobowe są gromadzone i przetwarzane w systemie rocznym w postaci elektronicznej (przy użyciu sprzętu komputerowego) lub w formie dokumentów biurowych, w zależności od ich rodzaju.
3. Administrator danych jest obowiązany czuwać nad tym, aby dane osobowe były merytorycznie poprawne, zbierane i przetwarzane zgodnie z prawem.
4. Odpowiedzialność za wykonywanie wynikających z ustawy obowiązków ponoszą reprezentanci.

5. Osobami uprawnionymi do gromadzenia i przetwarzania danych osobowych są:

- a) dyrektor szkoły,
- b) nauczyciele w przypadku danych związanych z uczniami, ich rodzicami (prawnymi opiekunami),
- f) inne osoby upoważnione pisemnie przez dyrektora.

§ 9

1. Administrator danych prowadzi listę osób zatrudnionych przy gromadzeniu i przetwarzaniu danych osobowych, stanowiącą załącznik nr 3 do Polityki bezpieczeństwa przetwarzania danych.

2. Osoby te są obowiązane zachować uzyskane informacje w tajemnicy, co potwierdzają własnoręcznym podpisem wraz ze złożeniem stosownego oświadczenia na odpowiednim formularzu, stanowiącym załącznik nr 6 do Polityki bezpieczeństwa przetwarzania danych. Oświadczenie to zostaje włączone do akt osobowych pracownika.

3. Ponadto każdy pracownik szkoły powinien wyrazić zgodę na zbieranie i przetwarzanie danych osobowych swoich i członków rodziny (pozostających we wspólnym gospodarstwie domowym), w zakresie spraw określonych w § 8 niniejszej instrukcji. Zgoda ta winna zostać wyrażona w oświadczeniu zgodnym z wzorem stanowiącym załącznik nr 6 do Polityki bezpieczeństwa przetwarzania danych, i podlega włączeniu do akt osobowych tego pracownika.

§ 10

1. Każdy nauczyciel szkoły, ma obowiązek zebrać oświadczenia woli od rodziców (prawnych opiekunów) swoich dzieci - uczniów, w których wyrażono zgodę na zbieranie i przetwarzanie danych osobowych zarówno tych dzieci, jak i ich prawnych opiekunów, w zakresie określonym w § 3 pkt. 1b niniejszej instrukcji.

2. Oświadczenie woli, o którym mowa w pkt. 1, winno być składane, przez co najmniej jednego z rodziców lub prawnych opiekunów, na odpowiednim formularzu.

V. Szczegółne zasady bezpieczeństwa

§ 11

1. Dane osobowe, są gromadzone i przechowywane w urządzeniach elektronicznych (komputerach, dyskieciech, płytach CD) a przede wszystkim w postaci akt.

2. Obszarem przetwarzania danych osobowych z użyciem sprzętu elektronicznego gabinet dyrektora, sale lekcyjne wyposażone w komputery lub laptopy nauczycielskie.

3. Administrator jest odpowiedzialny za zabezpieczenie zbiorów danych osobowych poprzez przeciwdziałanie dostępowi do informatycznych baz danych osób nieupoważnionych, a w szczególności za:

1) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkownika oraz kontroli dostępu do danych osobowych

2) podejmowanie odpowiednich działań w wypadku wykrycia naruszeń systemu.

§ 12

W pomieszczeniach, do których dostęp mają nieuprawnione osoby trzecie, monitorowany sposób, by uniemożliwić tym osobom wgląd w dane osobowe wyświetlane na ekranach tych urządzeń.

§ 13

Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia przechowuje się w warunkach uniemożliwiających dostęp do nich osobom trzecim.

§ 14

1. Klucze od pomieszczeń, w których wykonywane jest przetwarzanie danych osobowych, znajdują się w dyspozycji osób zatrudnionych przy przetwarzaniu danych i nie są udostępniane osobom postronnym, ani innym pracownikom administratora danych, za wyjątkiem personelu sprząającego i usuającego zaisiniące w tych pomieszczeniach awarie.

2. Przechowywanie w tych pomieszczeniach osób nieuprawnionych do zapoznania się z danymi osobowymi jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

§ 15

1. Dostęp do zbiorów danych osobowych znajdujących się na dyskach następuje wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

3. W razie przetwarzania pracy, przy urządzeniu powinien funkcjonować wyłącznik ekranu komputera.

4. W przypadku podejrzenia, iż wiadomość o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane powinna dokonać zmiany hasła, jednocześnie informując o tym niezwłocznie dyrektora szkoły.

5. Niezwłoczne powiadomienie dyrektora placówki, konieczne jest również, w razie stwierdzenia innego naruszenia systemów informatycznych, niż wymienione w pkt. 4.

§ 16

1. Wszystkie komputery biorące udział w przetwarzaniu danych osobowych winny być zabezpieczone przed nagłym zanikiem napięcia oraz niepowołanym dostępem.

2. Wszystkie komputery winny być systematycznie sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

3. Wszystkie hasła dostępowe do urządzeń powinny podlegać okresowej zmianie, dokonywanej z częstotliwością dostosowaną do rodzaju i znaczenia danych podlegających gromadzeniu i przetwarzaniu. Zmiana ta winna następować nie rzadziej niż raz w roku kalendarzowym.

1. Elektroniczne bazy danych osobowych winny być systematycznie archiwizowane.

2. Dane należy okresowo zapisywać i zabezpieczać, w sposób odpowiedni do skutecznego zabezpieczenia przed ich trwałą i nieodwracalną utratą.

3. Kopie danych winny być wykonywane na nośnikach magnetycznych i odpowiednio magazynowane, w sposób zapewniający ich bezpieczeństwo.

VI. Odpowiedzialność za naruszenie instrukcji

§ 18

Osoba przetwarzająca dane, która stwierdziła niebezpieczeństwo naruszenia przepisów instrukcji i nie poinformowała o tym dyrektora placówki w przypadku zaistnienia naruszenia postanowień wynikających z niniejszej instrukcji ponosić będzie odpowiedzialność odszkodowawczą wobec pracodawcy, na zasadach określonych w odrębnych przepisach.

VII. Zmiany instrukcji

§ 19

Wszelkie zmiany w powyższej instrukcji wprowadzane przez administratora danych skuteczne są wobec wszystkich osób, których dotyczą, z chwilą ich doręczenia tym osobom na piśmie.

VIII. Moc obowiązująca

§ 20

Niniejsza instrukcja zostaje wprowadzona zarządzeniem dyrektora szkoły i obowiązuje po upływie dwóch tygodni od dnia jej podpisania i wywieszenia na tablicy ogłoszeń.