Załącznik do zarządzenia nr 7/2015
Obowiązuje od 24.11.2015r.

POLITYKA BEZPIECZEŃSTWA

obowiązująca

w Zespole Szkół nr 4

w Nowym Sączu

Spis treści

Podstawa prawna

§ 1

- Konstytucja RP (art. 47 i 51).
- Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych 95/46/WE.
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 poz. 1182 ze zm.).
- 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. 2004 nr 100 poz. 1024 ze zm.).
- 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. 2008 nr 229 poz. 1536).
- Rozporządzenie Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej.
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. 2014 poz. 1934).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 poz. 719).

Podstawowe pojęcia

§ 2

W dokumencie przyjmuje się następującą terminologię:

- **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 Osobowych (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.
- **Administrator Systemu Informatycznego (ASI)** – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie.
- **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole.
- **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** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
- **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.
- **Szkoła** – Zespół Szkół nr 4 w Nowym Sączu.
- **Podmiot** – spółka prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostka budżetowa.
- **Polityka** – Polityka bezpieczeństwa obowiązująca w Zespole Szkół nr 4 w Nowym Sączu.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Wprowadzenie

§ 3

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Zespole Szkół nr 4 w Nowym Sączu, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 4

Administrator Danych Osobowych w podmiocie Dyrektora Szkoły wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych Osobowych sam wykonuje te czynności.

§ 5

Administrator Danych Osobowych wyznacza **Administratora Systemu Informatycznego** w celu nadzorowania funkcjonowania systemu informatycznego oraz stosowania technicznych środków ochrony stosowanych w tym systemie chyba, że Administrator Danych Osobowych przekazuje te czynności ABI.

2. Wykaz miejsc przetwarzania danych

§ 6

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do Polityki Bezpieczeństwa nr 1.**

3. Wykaz i opis struktury zbiorów danych osobowych

§ 7

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi określa **załącznik do Polityki Bezpieczeństwa nr 2.**

4. Sposób przepływu danych między poszczególnymi systemami

§ 8

Sposób przepływu danych między poszczególnymi systemami określa **załącznik do Polityki Bezpieczeństwa nr 3.**

5. Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

5.1. Deklaracja intencji, cele i zakres polityki bezpieczeństwa

§ 9

Administrator Danych Osobowych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.

§ 10

Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.

§ 11

Polityka dotyczy wszystkich danych osobowych przetwarzanych w Szkole, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

§12

Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

§ 13

Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w Szkole oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

§ 14

Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza Polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

§ 15

Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:

- **a)** poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
- **b)** integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
- **c)** dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot
- **d)** rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
- **e)** autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
- **f)** niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
- **g)** niezawodność – zamierzone zachowania i skutki są spójne.

5.2. Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 16

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

§ 17

Administrator Danych Osobowych (ADO):

- **a)** formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- **b)** decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- **c)** odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole,
- **d)** zapewnia, aby dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

§ 18

Administrator Bezpieczeństwa Informacji (ABI):

- **a)** egzekwuje zgodnie z prawem przetwarzanie danych osobowych w Szkole w imieniu ADO,
- **b)** wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa **załącznik do Polityki Bezpieczeństwa nr 4**,
- **c)** wydaje unieważnienia upoważnienia do przetwarzania danych osobowych – wzór unieważnienia określa **załącznik do Polityki Bezpieczeństwa nr 5**,
- **d)** prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych – wzór wykazu osób upoważnionych do przetwarzania danych określa **załącznik do Polityki Bezpieczeństwa nr 6**,
- **e)** określa potrzeby w zakresie stosowanych w Szkole zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,
- **f)** udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
- **g)** bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnia odpowiedni poziom przeszkolenia w tym zakresie,

h) prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w Szkole wynikającą z przepisów prawa.

§ 19

Administrator Systemu Informatycznego (ASI):

a) zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI,

b) doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,

c) przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,

d) nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,

e) zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,

f) prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§ 20

Pracownik przetwarzający dane:

a) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły i składa oświadczenie o znajomości tych przepisów – wzór potwierdzenia znajomości zasad bezpieczeństwa określa **załącznik do Polityki Bezpieczeństwa nr 7**,

b) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez ADO lub ABI w upoważnieniu i tylko w celu wykonania nałożonych obowiązków,

c) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania,

d) stosuje określone przez ADO oraz ABI procedury oraz wytyczne mające na celu zgodnie z prawem, w tym zwłaszcza adekwatnie, przetwarzanie danych,

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

f) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

5.3. Zasady udzielania dostępu do danych osobowych

§ 21

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Szkole Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu. Potwierdzenie znajomości zasad bezpieczeństwa włącza się do akt osobowych danego pracownika Szkoły.

§ 22

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ABI.

§ 23

ABI może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników Szkoły do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Szkole.

5.4. Udostępnianie i powierzanie danych osobowych

§ 24

Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 25

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

a) adresat wniosku (administrator danych),
b) wnioskodawca,
c) podstawa prawna (wskazanie potrzeby),
d) wskazanie przeznaczenia,
e) zakres informacji.

§ 26

Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 27

Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna precyzyjnie określać zakres danych przekazanych do przetwarzania oraz informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 28

Podmiot, któremu powierzono przetwarzanie może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 29

Podmiot przetwarzający dane na zlecenie ma obowiązek przed rozpoczęciem przetwarzania zabezpieczyć dane oraz spełnić wymagania określone w przepisach wykonawczych (tj. w szczególności prowadzić dokumentację, czyli politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym).

§ 30

Odpowiedzialność za przestrzeganie ustawy o ochronie danych osobowych spoczywa na ADO, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

§ 31

Każda osoba fizyczna, której dane przetwarzane są w Szkole, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w *art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych* prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 32

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ADO, udzielając informacji o zawartości zbioru danych na piśmie.

5.5. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 33

Przetwarzanie danych osobowych w Szkole może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.

§ 34

Zabrania się przetwarzania danych poza obszarem określonym w załączniku nr 1 do niniejszej Polityki.

§ 35

Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą ABI lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nieposiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio **załącznik nr 8** oraz **załącznik nr 9 do Polityki Bezpieczeństwa**.

§ 36

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

§ 37

Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych, przy czym arkusze ocen są wydawane osobom uprawnionym przez wyznaczonego do tego celu pracownika.

§ 38

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ADO w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

§ 39

W obszarach przetwarzania danych obowiązuje zakaz korzystania z urządzeń rejestrujących obraz lub dźwięk.

§ 40

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.

5.6. Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§ 41

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w *Instrukcji zarządzania systemem informatycznym*, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Szkoły.

6. Analiza ryzyka związanego z przetwarzaniem danych osobowych

6.1. Charakterystyka możliwych zagrożeń

§ 42

W przypadku danych przetwarzanych w sposób tradycyjny możemy wyróżnić następujące zagrożenia:

- → oszustwo, kradzież, sabotaż;
- → zdarzenia losowe (np. powódź, pożar);
- → zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej);
- → niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;
- → pokonanie zabezpieczeń fizycznych;

- podsłuchy, podglądy;
- brak rejestrowania udostępniania danych;
- niewłaściwe miejsce i sposób przechowywania dokumentacji.

§ 43

W przypadku danych przetwarzanych w systemach informatycznych możemy wyróżnić następujące zagrożenia:

- nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów;
- niewłaściwa administracja systemem;
- niewłaściwa konfiguracja systemu;
- zniszczenie (sfałszowanie) kont użytkowników;
- kradzież danych kont;
- pokonanie zabezpieczeń programowych;
- zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej);
- niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;
- zdarzenia losowe (np. powódź, pożar);
- niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania za pomocą nośników informacji i komputerów przenośnych;
- naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione;
- przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci;
- przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci;
- przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych;
- brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

6.2. Sposób zabezpieczenia danych

§ 44

W przypadku danych przetwarzanych w sposób tradycyjny zastosowane są następujące sposoby zabezpieczeń:

- przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe;
- przechowywanie danych osobowych w szafach zamykanych na klucz;
- zastosowanie czujników ruchu informujących firmę ochroniarską o nieautoryzowanym wejściu do budynku;
- zastosowanie monitoringu wizyjnego (*dostęp do zapisu z monitoringu posiada ADO i ABI*);

- → przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez ADO lub ABI;
- → zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania.

§ 45

W przypadku danych przetwarzanych w systemach informatycznych zastosowane są następujące sposoby zabezpieczeń:

- → kontrola dostępu do systemów;
- → zastosowanie programów antywirusowych, zapór ogniowych (firewall) i innych regularnie aktualizowanych narzędzi ochrony;
- → stosowanie ochrony zasilania;
- → systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;
- → składowanie danych wrażliwych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach;
- → przydzielenie pracownikom indywidualnych kont użytkowników i haseł;
- → stosowanie indywidualnych haseł logowania do poszczególnych programów;
- → właściwa budowa hasła.

6.3. Określenie wielkości ryzyka

§ 46

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

7. Instrukcja postępowania w sytuacji naruszenia danych

7.1. Istota naruszeń danych osobowych

§ 47

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- **a)** nieautoryzowany dostęp do danych,
- **b)** nieautoryzowane modyfikacje lub zniszczenie danych,
- **c)** udostępnienie danych nieautoryzowanym podmiotom,

d) nielegalne ujawnienie danych,
e) pozyskiwanie danych z nielegalnych źródeł.

7.2. Sytuacje świadczące o naruszeniu zasad bezpieczeństwa

§ 48

Sytuacje świadczące o naruszeniu zasad bezpieczeństwa:

a) **przełamane zabezpieczeń tradycyjnych** (np. zerwane plomby na drzwiach, szafach, segregatorach, uszkodzone zamki w drzwiach, szafach),
b) **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych** na zasoby systemu (np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej),
c) **niewłaściwe parametry środowiska**, (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych),
d) **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,
e) **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
f) **jakość danych w systemie** lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
g) **naruszenie lub próba naruszenia integralności** systemu lub bazy danych w tym systemie,
h) **próba lub modyfikacja danych** oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
i) **niedopuszczalna manipulacja** danymi osobowymi w systemie,
j) **ujawnienie osobom nieupoważnionym danych osobowych** lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu,
k) **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),
l) **ujawnienie istnienia nieautoryzowanych kont dostępu** do danych,
m) **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych,
n) **rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, prace na danych osobowych w celach prywatnych).

7.3. Postępowanie w przypadku naruszenia danych osobowych

§ 49

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ABI lub ADO.

§ 50

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

§ 51

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.

§ 52

ABI podejmuje następujące kroki:

- **a)** zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Szkoły,
- **b)** może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- **c)** powiadamiania o zaistniałym naruszeniu ADO,
- **d)** nawiązuje kontakt ze specjalistami spoza Szkoły (jeśli zachodzi taka potrzeba).

§ 53

ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego **załącznik nr 10 do Polityki Bezpieczeństwa** i przekazuje go ADO.

§ 54

ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

7.4. Sankcje karne

§ 55

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

§ 56

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

1. Wprowadzenie

§ 57

W związku z tym, że w Szkole przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim**.

2. Ogólne zasady pracy w systemie informatycznym

§ 58

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
- → poprzez zainstalowanie programu antywirusowego
- → poprzez zainstalowanie firewall (zapora sieciowa)
- → poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem

b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

§ 59

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.

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

§ 60

Użytkowników systemu informatycznego tworzy oraz usuwa ASI na podstawie zgody ADO.

§ 61

Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.

§ 62

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.

§ 63

Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

§ 64

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.

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

§ 65

System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

§ 66

Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator.

§ 67

W identyfikatorze pomija się polskie znaki diakrytyczne.

§ 68

Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz identyfikatora i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy.

§ 69

Hasło nadane przez użytkownika musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

§ 70

Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni.

§ 71

Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

§ 72

Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

§ 73

Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,

b) aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

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

§ 74

Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

§ 75

Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.

§ 76

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.

§ 77

Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem §76.

§ 78

Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.

§ 79

ASI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

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

§ 80

Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.

§ 81

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.

§ 82

Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.

§ 83

Odpowiedzialnym za wykonanie kopii zapasowych jest użytkownik obsługujący dany program przetwarzający dane.

§ 84

Kopie zapasowe mogą być wykonywane tylko na nośnikach informatycznych dostarczonych przez ASI.

§ 85

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

§ 86

Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 87

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.

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

§ 88

Kopie zapasowe sporządzone na nośnikach informatycznych przechowuje pracownik tworzący te kopie w odpowiednio zabezpieczonym miejscu.

§ 89

Dane osobowe gromadzone są na stacjach roboczych oraz na nośnikach zewnętrznych.

§ 90

Przenośne nośniki danych zabezpieczone są hasłem.

§ 91

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

a) **likwidacji** – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
b) **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) **naprawy** – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ABI.

§ 92

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

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

§ 93

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

a) skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.
b) automatycznej aktualizacji bazy wirusów.

§ 94

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

§ 95

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI 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.

§ 96

Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

9. Charakterystyka systemu przetwarzającego dane osobowe

§ 97

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych

wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu,

b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

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

d) informacji o odbiorcach, w rozumieniu *art. 7 pkt 6 ustawy o ochronie danych osobowych*, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

e) sprzeciwu wobec przetwarzania danych w przypadkach, wymienionych w *art. 23 ust. 1 pkt 4 i 5 ustawy o ochronie danych osobowych*, gdy Administrator Danych Osobowych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania danych osobowych innemu administratorowi danych.

§ 98

Odnotowanie informacji, o których mowa w §97, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

§ 99

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w §97.

§ 100

W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w §97 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

10. Przesyłanie danych poza obszar przetwarzania

§ 101

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.

§ 102

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 transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych,
d) umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

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

§ 103

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w Szkole oraz dbać o ich dobry stan techniczny.

§ 104

Przeglądy o których mowa w §103 może wykonywać też osoba powołana przez ABI.

§ 105

Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych Administrator Bezpieczeństwa Informacji ma obowiązek niezwłocznie powiadomić o tym fakcie ADO.

§ 106

W przypadku stwierdzenia przez ABI uchybień dotyczących przetwarzania danych w Szkole powinien o tym fakcie niezwłocznie powiadomić ADO oraz wprowadzić odpowiednie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

Postanowienia końcowe

§ 107

W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie odpowiednie przepisy *ustawy o ochronie danych osobowych* oraz *Rozporządzenia Ministra Spraw Wewnętrznych i Administracji* w *sprawie dokumentacji przetwarzania danych osobowych, oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*.

Załączniki

Załącznik nr 1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Załącznik nr 2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Załącznik nr 3. Sposób przepływu danych między poszczególnymi systemami.

Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

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

Załącznik nr 6. Wzór wykazu osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 7. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

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

Załącznik nr 9. Wzór odwołania zgody na przebywanie w obszarze przetwarzania danych osobowych.

Załącznik nr 10. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.

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

Lp.	Nazwa pomieszczenia	Adres
1	Gabinet Dyrektora	ul. Św. Ducha 6, 33-300 Nowy Sącz
2	Gabinet Wicedyrektora	ul. Św. Ducha 6, 33-300 Nowy Sącz
3	Gabinet Kierownika	ul. Św. Ducha 6, 33-300 Nowy Sącz
4	Sekretariat	ul. Św. Ducha 6, 33-300 Nowy Sącz
5	Księgowość	ul. Św. Ducha 6, 33-300 Nowy Sącz
6	Pokój nauczycielski	ul. Św. Ducha 6, 33-300 Nowy Sącz
7	Gabinet pedagoga i psychologa	ul. Św. Ducha 6, 33-300 Nowy Sącz
8	Gabinet nauczycieli wychowania fizycznego	ul. Św. Ducha 6, 33-300 Nowy Sącz
9	Sale dydaktyczne: 1 – przedsiębiorczości 2 – języka niemieckiego 3 – gimnastyczna 10 – religijna 12 – historyczna 13 – fizyczno-chemiczna 14 – języka angielskiego 16 – polonistyczna 17 – biologiczna 18 – informatyczna 19 – informatyczna 20 – zawodowa 21 – zawodowa 27 – matematyczna 26 – polonistyczna	ul. Św. Ducha 6, 33-300 Nowy Sącz

	11 – języka angielskiego 15 – języka angielskiego 28 – językowa 29 – fryzjerska	
10	Biblioteka	ul. Św. Ducha 6, 33-300 Nowy Sącz

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Lp.	Nazwa zbioru	Struktura zbioru	Programy zastosowane do przetwarzania danych
1	Dane pracowników	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres, pesel, wykształcenie, przebieg dotychczasowego zatrudnienia, daty urodzenia dzieci, imiona i nazwiska dzieci, orzeczenie o stanie zdrowia, wymiar uposażenia, ukończone kursy i szkolenia, kary i nagrody, zapytanie o udzielenie informacji o osobie, umowy, zaświadczenie BHP	Kadry Optivum
2	Awans zawodowy	Imię i nazwisko, data urodzenia, adres, przebieg zatrudnienia, wykształcenie, składniki wynagrodzenia	
3	System informacji Oświatowej *(stary)*	Pesel, rok urodzenia, stopień awansu, staż pracy, wynagrodzenie, kwalifikacje, płeć	SIO *(stary)*
4	System informacji Oświatowej *(nowy)*	Imię i nazwisko, pesel, stopień awansu, staż pracy, wynagrodzenie, kwalifikacje, stanowisko, zatrudnienie	SIO *(nowy)*
5	Ubezpieczenie ZUS	Imię i nazwisko, data urodzenia, adres, pesel, NIP, wynagrodzenie	Płatnik
6	Dobrowolne ubezpieczenie pracowników	Imię i nazwisko, data i miejsce urodzenia, adres, pesel, obywatelstwo, uposażeni (imię i nazwisko, data i miejsce urodzenia, adres, procent świadczenia)	ERU PZU
7	Umowy zlecenia	Imię i nazwisko, adres, pesel, NIP, seria i nr dowodu osobistego, telefon, imiona rodziców, nr rachunku bankowego, data i miejsce urodzenia	Finanse Optivum
8	Przelewy	Imię i nazwisko, adres, nr rachunku bankowego, NIP	Bank ING
9	Faktury	Imię i nazwisko, adres, NIP	Finanse Optivum
10	Pity	Imię i nazwisko, adres, NIP, pesel, dochody	
11	Podania o pracę	Imię i nazwisko, adres, telefon, e-mail,	

		wykształcenie	
12	Dziennik korespondencji	Imię i nazwisko, adres	
13	Arkusz organizacyjny	Imię i nazwisko, pesel, data urodzenia, poziom wykształcenia, stopień awansu zawodowego, staż pracy, wniosek o postępowanie kwalifikacyjne/ egzaminacyjne, ukończone studia, przygotowanie pedagogiczne, data rozpoczęcia stażu na wyższy stopień, specjalności nauczyciela	Arkusz Optivum
14	Rozkład zajęć	Imię i nazwisko, e-mail	Plan Lekcji Optivum
15	Świadczenia socjalne	Imię i nazwisko, adres zamieszkania lub pobytu, dochody brutto, ilość osób w rodzinie, telefon, stan zdrowia	
16	Dokumentacja powypadkowa pracowników	Imię i nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, stan zdrowia, imię ojca, opis wypadku	
17	Monitoring wizyjny	Wizerunek osoby (postać , sylwetka)	
18	Protokoły Rady Pedagogicznej	Imię i nazwisko, przydział dodatkowych czynności	
19	Księga zastępstw	Imię i nazwisko	
20	Księga ewidencji uczniów	Imię i nazwisko, data i miejsce urodzenia, adres, pesel, profil klasy, przyjęcie do szkoły: data, klasa, semestr, wypisanie ze szkoły: data, klasa, data wydania świadectwa, numer świadectwa, imiona rodziców i adres	
21	Rekrutacja	Imię i nazwisko, data i miejsce urodzenia, adres, pesel, imię rodziców, telefon	
22	Ubezpieczenie uczniów	Imię i nazwisko, klasa	
23	Arkusz ocen	Imię i nazwisko, data i miejsce urodzenia, adres, pesel, nr księgi ewidencji uczniów, profil klasy, wyniki nauki, imię i nazwisko rodziców, telefon, adres	
24	Świadectwa	Imię i nazwisko, data i miejsce urodzenia, uzyskane oceny, pesel, data wydania	Świadectwa Optivum
25	Potwierdzenie odbioru świadectw	Imię i nazwisko, klasa	
26	Ewidencja legitymacji szkolnych	Imię i nazwisko, klasa	
27	Dziennik lekcyjny	Imię i nazwisko ucznia, data urodzenia,	

		miejsce urodzenia, miejsce zamieszkania lub pobytu, pesel, numer ewidencyjny ucznia, imiona i nazwiska rodziców, telefon, adres zamieszkania, który rok w klasie, opinie poradni, informacje o wynikach w nauce	
28	Dziennik zajęć pozalekcyjnych	Imię i nazwisko ucznia, data urodzenia, adres zamieszkania, numer ewidencyjny ucznia, imiona i nazwiska rodziców, telefon	
29	Dziennik indywidualnego nauczania	Imię i nazwisko ucznia, adres zamieszkania, imiona i nazwiska rodziców, telefon, informacje o wynikach w nauce	
30	Dokumentacja powypadkowa uczniów	Imię i nazwisko ucznia, data urodzenia, adres zamieszkania lub pobytu, klasa, szkoła, opis wypadku	
31	Duplikaty dokumentacji uczniów	Imię i nazwisko, data i miejsce urodzenia, szkoła, informacje o wynikach w nauce	
32	Wycieczki	Imię i nazwisko, adres, pesel, telefon, klasa	
33	Arkusz dostosowania wymagań	Imię i nazwisko dziecka, adres zamieszkania dziecka, data urodzenia, miejsce urodzenia, imiona rodziców, numer opinii lub orzeczenia informacje dot. rozwoju dziecka, formy dostosowania wymagań, zalecenia poradni	
34	Wyprawka szkolna	Imię i nazwisko ucznia, data urodzenia, miejsce urodzenia, adres zamieszkania, imiona i nazwiska rodziców, adres zamieszkania rodziców, PESEL rodzica i dziecka, dochód	
35	Stypendia	Imię i nazwisko	
36	Dokumentacja Pedagoga	Imię i nazwisko, data urodzenia, adres, stan zdrowia, opinie poradni, sytuacja rodzinna ucznia, inne dane o uczniu zebrane ze źródeł trzecich	
37	Opinie i Orzeczenia Poradni Psychologiczno-Pedagogicznej	Imię i nazwisko, data urodzenia, stan zdrowia, zalecenia, formy pomocy	
38	Biblioteka	Imię i nazwisko, klasa, szkoła, adres, telefon, dane o wypożyczeniach	MOL Optivum

Sposób przepływu danych między poszczególnymi systemami

Lp.	Źródłowy system informatyczny	Docelowy system informatyczny	Zakres przesyłanych danych	Sposób transmisji
	SIO (lokalny)	SIO (zewnętrzny)	Dane nauczycieli	Poprzez sieć teleinformatyczną
	Płatnik (sekretariat)	Płatnik (księgowość)	Dane zgłoszeniowe	Manualny
	Płatnik (księgowość)	ZUS	Dane pracowników	Poprzez sieć teleinformatyczną
	Płace	Urząd Skarbowy	Pity	Poprzez sieć teleinformatyczną
	Płace	Bank ING	Dane pracowników	Poprzez sieć teleinformatyczną
	Płace	SIO (lokalny)	Dane pracowników	Manualny
	Płace	Płatnik	Informacja o składkach ZUS	Manualny
	Płatnik	ZUS	Składki ZUS	Poprzez sieć teleinformatyczną
	Płace	Bank ING	Podatek	Poprzez sieć teleinformatyczną
	Płace	SIGMA	Wynagrodzenia nauczycieli	Poprzez sieć teleinformatyczną
	Finanse Optivum	SIO	Bilanse	Manualny
	Finanse Optivum	SIGMA	Sprawozdania	Poprzez sieć teleinformatyczną
	ERU PZU (lokalny)	ERU PZU (zewnętrzny)	Dane pracowników	Poprzez sieć teleinformatyczną
	Arkusz Optivum	Plan Lekcji Optivum	Dane pracowników	Manualny

Pozostałe programy są niezależne i posiadają samodzielne bazy danych.

……., dn. …….

……

(sygnatura)

WAŻNOŚĆ

od: ……

do: ……

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:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

……

……

……

……

Administrator Bezpieczeństwa Informacji

……., dn. …….

……

(sygnatura)

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 dnia ……. o sygnaturze …… dla Pani/Pana:

……

……

Administrator Bezpieczeństwa Informacji

Wzór wykazu osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko służbowe	Numer zbiorów danych	Okres upoważnienia		Identyfikator *(jeśli dane są przetwarzane w systemie informatycznym)*
				OD	DO	

……., dn. …….

…….
(imię i nazwisko pracownika)

OŚWIADCZENIE

1. Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w Zespole Szkół nr 4 w Nowym Sączu w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" oraz respektowania zapisów Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w Zespole Szkół nr 4 oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

2. Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, 1662) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 ze zm.).

3. Oświadczam, że zostałem(am) poinformowany(a) o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w Zespole Szkół nr 4 może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

……
(podpis pracownika)

……., dn. …….

……

(sygnatura)

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.

……

Administrator Bezpieczeństwa Informacji

……., dn. …….

……

(sygnatura)

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.

……
Administrator Bezpieczeństwa Informacji

RAPORT

z naruszenia bezpieczeństwa zasad ochrony danych osobowych

w ……

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

2. Osoba powiadamiająca o zaistniałym zdarzeniu:
……
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika)

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:
……
……
……

……
Administrator Bezpieczeństwa Informacji