POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH
W ZESPOLE SZKÓŁ W RADZYNIU CHEŁMIŃSKIM

Zatwierdził (data i podpis): 02.01.2013

Rejestr zmian w dokumencie:

Wersja	Data	Opracował	Opis nowelizacji

Dokumenty powiązane:

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół w Radzyniu Chełmińskim

§ 1

Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Zespole Szkół w Radzyniu Chełmińskim zwana dalej „Polityką", została wydana w związku z § 3 ust. 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 (Dz. U. Nr 100, poz. 1024).
2. W dalszej części Polityki Zespół Szkół w Radzyniu Chełmińskim nazywany będzie Zespołem Szkół.
3. Celem Polityki jest stworzenie podstaw dla właściwego wykonania obowiązków Administratora Danych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych.
4. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Zespołu Szkół oraz w kontaktach z otoczeniem społecznym.
5. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
6. Niniejszą Politykę stosuje się do:
   1) Danych osobowych:
      a. przetwarzanych w systemach informatycznych i nieinformatycznych,
      b. zapisanych się na zewnętrznych nośnikach informacji,
   2) Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:
      a. służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
      b. dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
7. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe, których administratorem jest Zespół Szkół lub które są przetwarzane przez podmioty trzecie na podstawie umów powierzeń, o których mowa w art. 31 Ustawy.

§ 2

Definicje

1. Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte w Zespole Szkół.

1. **Administrator Danych**, podmiot który decyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez dyrektora Zespołu Szkół.
2. **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez dyrektora, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
3. **Administratorzy Systemu** – wyznaczone osoby, odpowiedzialne za funkcjonowanie infrastruktury informatycznej na którą składa się sprzęt informatyczny oraz systemy i aplikacje informatyczne, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.
4. **Bezpieczeństwo przetwarzania danych osobowych** - zachowanie poufności, integralności i rozliczalności danych osobowych; dodatkowo, mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
5. **Dyrekcja** – dyrektor oraz wicedyrektorzy.
6. **Dane Osobowe** - każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikacje tej osoby.
7. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
8. **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
9. **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie ochrony danych osobowych.
10. **Poufność** – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym.
11. **Przetwarzanie danych osobowych** - 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.
12. **Rozporządzenie** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakie powinny spełniać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
13. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
14. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
15. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

16. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
17. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
18. **Zbiór nieinformatyczny** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

§ 3

Deklaracja dyrekcji

2. Dyrekcja zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:
   1) Przetwarzane zgodnie z prawem.
   2) Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
   3) Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
   4) Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
   5) Zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych.
3. Przy przetwarzaniu danych osobowych w systemach informatycznych Zespołu Szkół należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia.

§ 4

Przegląd dokumentacji z zakresu ochrony danych osobowych

4. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Zespołu Szkół, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
5. Przegląd Polityki ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Zespołu Szkół oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.
6. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych.
7. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Zespole Szkół dotyczących ochrony danych osobowych.
8. Wszelkie zmiany Polityki powinny być zatwierdzane przez dyrektora Zespołu Szkół.

§ 5

Zarządzanie ochroną danych osobowych

9. Realizację zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:
   1) Przeszkolenie użytkowników w zakresie bezpieczeństwa przetwarzania danych osobowych.
   2) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.
   3) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.
   4) Podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych.
   5) Śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.
10. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.
11. Dyrekcja powinna uzyskać zapewnienie, że pracownicy oraz użytkownicy reprezentujący stronę trzecią:
   1) Są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych.
   2) Otrzymują zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami w Zespole Szkół.
   3) Wypełniają zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy.
   4) W sposób ciągły utrzymują odpowiednie umiejętności i kwalifikacje.
12. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.

§ 6

Odpowiedzialność Dyrekcji

1. Dyrekcja jest odpowiedzialna za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Dyrektora należy w szczególności:
   1) Wyznaczenie Administratora Bezpieczeństwa Informacji.

2) Określenie celów i strategii ochrony danych osobowych.

3) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

4) Określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych.

5) Określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych).

6) Ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.

3. Do obowiązków Dyrektora należy:

1) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem.

2) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Zespole Szkół.

3) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.

4) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych.

5) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.

6) Zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

7) Zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia.

8) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.

9) Zapewnienie dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w Rozporządzeniu.

10) Realizację obowiązku informowania o przetwarzaniu danych osobowych, osób, których dane osobowe są pozyskiwane.

11) Zapewnienie na żądanie uprawnionych osób, udostępniania informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.

12) Zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych.

13) Zapewnienie uzyskania przez pracowników przetwarzających dane osobowe, formalnego upoważnienia do przetwarzania danych osobowych.

14) W przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje powinny zostać przekazane do Administratora Bezpieczeństwa Informacji.

§ 7

Odpowiedzialność Administratora Bezpieczeństwa Informacji

1. Dyrektor wyznacza Administratora Bezpieczeństwa Informacji, który nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej. W przypadku nie wyznaczenia Administratora Bezpieczeństwa Informacji, jego zadania wykonuje Dyrektor.
2. Do kompetencji Administratora Bezpieczeństwa Informacji należy:
   1) Określenie zasad ochrony danych osobowych.
   2) Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.
3. Do obowiązków Administratora Bezpieczeństwa Informacji należy:
   1) Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych.
   2) Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych.
   3) Prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury) oraz zapewnienie ich publikacji i dystrybucji.
   4) Zapoznawanie pracowników oraz współpracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.
   5) Reprezentowanie Zespołu Szkół w kontaktach z Biurem GIODO.
   6) Przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO.
   7) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń.
   8) Sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.
   9) Prowadzenie pełnej dokumentacji związanej z ochroną danych osobowych, zawierającej:
      c. ewidencję zbiorów danych osobowych,
      d. ewidencję osób upoważnionych do przetwarzania danych osobowych,
      e. wykaz obszarów przetwarzania danych osobowych,
      f. dokumenty z audytów i przeglądów bezpieczeństwa,
      g. oryginały i kopie dokumentów dotyczących ochrony danych osobowych, w szczególności uchwały Zarządu, polityki bezpieczeństwa, instrukcje, regulaminy, procedury,
      h. programy szkoleń, listę przeszkolonych osób,
      i. kopie wniosków o rejestrację zbiorów,
      j. raport z wypełnienia obowiązku informacyjnego (kopie wniosków, pism z klauzulami informacyjnymi).
4. Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska, udzielania natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych,

które może skutkować postawieniem Dyrektora popełnienia jednego z przestępstw, wskazanych ww. Rozdziale 8 Ustawy.

5. Sprawowanie nadzoru nad przestrzeganiem zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym osobowym odpowiednią do zagrożeń oraz kategorii danych objętych ochroną powinno być głównym zadaniem Administratora Bezpieczeństwa Informacji.

§ 8

Odpowiedzialność pracowników i użytkowników systemu

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika w zakresie ochrony danych osobowych.
2. Pracownicy Zespołu Szkół są zobowiązani do:
   1) Postępowania zgodnie z Polityką.
   2) Informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.
   3) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.
   4) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.
   5) Wykonywania konkretnych działań i procesów w celu zapewnienia ochrony danych osobowych.
3. Pracownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:
   1) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.
   2) Informować Administratora Bezpieczeństwa Informacji lub pracowników ochrony o podejrzanych osobach, tj.: osobach zachowujących się w sposób podejrzany np. nieodpowiednio ubranych do pory roku, dnia i pogody
4. Pracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§ 9

Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika, może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art. 266 Kodeksu Karnego. W takim przypadku zgodnie z przepisem art. 66 Kodeksu Pracy umowa o pracę z pracownikiem tymczasowo aresztowanym wygasa z upływem 3 miesięcy nieobecności pracownika w pracy z powodu tymczasowego aresztowania, chyba że pracodawca rozwiąże wcześniej bez wypowiedzenia umowę o pracę z winy pracownika.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Dyrektor nadaje charakter poufny

mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.

3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzecznych z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych) czy też ich przetwarzania w sposób niezgodny z przyjętymi w Zespole Szkół procedurami może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami Dyrektor może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.
5. Sankcje dotyczące ujawnienia poufnych danych osobowych stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w Zespole Szkół.

§ 10

Obowiązek informacyjny

13. W przypadku zbierania danych osobowych na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) należy umieszczać na nich odpowiednią klauzulę informacyjną. Klauzula taka powinna informować osobę, której dane zbieramy o:
    1) Adresie siedziby i pełnej nazwie Zespołu Szkół
    2) Celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych.
    3) Prawie dostępu do treści swoich danych oraz ich poprawiania.
    4) Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
14. Przepisu określonego w ust. 1 nie stosuje się, jeżeli:
    1) Przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.
    2) Osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1
15. Przepisu określonego w ust. 1 nie stosuje się w przypadkach określonych w art. 25 ust. 2 pkt 1, 3 i 5 Ustawy.

§ 11

Szkolenia w zakresie ochrony danych osobowych

16. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien zostać przeszkolony przez Administratora Bezpieczeństwa Informacji. Szkolenie powinno obejmować następujące zagadnienia:
    1) Przepisy o ochronie danych osobowych.
    2) Zasady przetwarzania danych osobowych.
    3) Procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych.
    4) Zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

5) Zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych.

6) Zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe.

7) Sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego.

8) Odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

17. Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.

18. Użytkownicy reprezentujący osoby trzecie (tam, gdzie jest to wskazane) powinni przechodzić przeszkolenie w zakresie:

1) Odpowiednich zasad wynikających z Polityki.

2) Odpowiednich procedur dotyczących bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych.

3) Poprawnego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

§ 12

Wymiana informacji dotyczących danych osobowych

19. Pracownicy Zespołu Szkół w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:

1) Wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi.

2) Ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem.

3) Zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywania poczty elektronicznej na zewnątrz.

4) Zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione.

5) Upewnienie się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych.

6) Zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione.

7) Nie pozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach.

8) Właściwe postępowanie z faksami i fotokopiarkami, ponieważ mają one podręczną pamięć i przechowują w niej strony zawierające np. dane osobowe na wypadek błędów transmisji.

20. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskania i odczyt przez osoby nieupoważnione.

§ 13

Przetwarzanie danych osobowych w obszarach bezpiecznych

21. Dane osobowe w Zespole Szkól mogą być przetwarzane w pomieszczeniach przetwarzania danych osobowych. Wyjątkiem jest przetwarzanie przez nauczycieli danych w zakresie dziennika elektronicznego, które mogą być przetwarzane na komputerach domowych pod warunkiem zachowania warunków określonych w Polityce oraz Instrukcji przetwarzania danych w systemach informatycznych.
22. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Zespół Szkół prowadzi działalność.
23. Do pomieszczeń przetwarzania danych osobowych zalicza się:
    1) Serwerownia.
    2) Pomieszczenia biurowe, w których zlokalizowane są stacje robocze.
    3) Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe.
    4) Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego.
    5) Pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.
    6) Pokoje nauczycielskie i pomieszczenia dydaktyczne.
24. Przebywanie wewnątrz obszarów, o których mowa w ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Dyrektora.
25. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp do nich osobom nieupoważnionym.
26. W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić:
    1) Jasne określenie granic obszaru przetwarzania danych osobowych oraz umiejscowienie dostosowane do wymagań bezpieczeństwa w odniesieniu do aktywów znajdujących się wewnątrz obszaru.
    2) Jednolite granice budynków lub pomieszczeń, gdzie zlokalizowano środki przetwarzania danych osobowych (tzn. aby granice nie miały luk lub punktów, przez które łatwo się włamać).
    3) Ściany zewnętrzne pomieszczeń solidnej konstrukcji oraz wszystkie drzwi zewnętrzne odpowiednio zabezpieczone przed nieautoryzowanym dostępem za pomocą mechanizmów zabezpieczeń, np. alarmów, zamków itp.
    4) Zamykanie drzwi i okien w pomieszczeniach.
    5) System wykrywania włamań zgodnych z normami w strefach bezpieczeństwa (np. serwerownia) oraz regularne jego testowanie.
27. Ochrona obszarów bezpiecznych powinna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające, że tylko osoby upoważnione mogą uzyskać dostęp, w tym celu należy zapewnić:
    1) Nadzorowanie pobytu osób nie będących pracownikami Zespole Szkół w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany.
    2) Kontrolowanie i ograniczenie dostępu do obszarów, gdzie są przetwarzane dane osobowe tylko dla uprawnionego personelu.

3) Regularne przeglądanie praw dostępu do obszarów bezpiecznych i jeśli zachodzi potrzeba, uaktualnianie ich lub odbieranie.

28. Nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

29. Każdorazowe uchybienie zabezpieczeń fizycznych chroniących dane osobowe powinno być zgłaszane do Administratora Bezpieczeństwa Informacji.

§ 14

Dopuszczenie osób do przetwarzania danych osobowych

30. Dyrekcja upoważniona jest do przetwarzania danych osobowych, których Administratorem Danych jest Zespół Szkół oraz danych osobowych, które są przetwarzane na podstawie art. 31 Ustawy.

31. Każda osoba po wejściu w skład Dyrekcji zobowiązana jest zapoznać się z Ustawą oraz niniejszą Polityką i dokumentami powiązanymi.

32. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika formalnego upoważnienia do przetwarzania danych osobowych wystawianego przez Administratora Bezpieczeństwa Informacji, w tym celu przełożony pracownika przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:

    1) Zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Zespole Szkół.

    2) Przyjmuje od pracownika podpisane oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z przepisami oraz oświadczenia o znajomości niniejszego dokumentu a także o znajomości „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół", którego wzór stanowi **załącznik nr 1** niniejszej Polityki.

    3) Wnioskuje do Administratora Bezpieczeństwa Informacji o formalne upoważnienie pracownika do przetwarzania danych osobowych sporządzane wg wzoru stanowiącego **załącznik nr 2** niniejszej Polityki.

33. Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika.

34. Przełożony pracownika jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika, złożyć rezygnację do Administratora Bezpieczeństwa Informacji dotyczącą jego dostępu do danych osobowych.

§ 15

Ewidencja osób upoważnionych do przetwarzania danych osobowych

35. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzania danych osobowych (ewidencja) powinna być prowadzona przez Administratora Bezpieczeństwa Informacji i powinna zawierać:

    1) Imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych.

    2) Zakres upoważnienia do przetwarzania danych osobowych.

    3) Wskazanie zajmowanego stanowiska osoby upoważnionej.

    4) Identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych.

    5) Datę nadania i odebrania uprawnień.

36. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.
37. Przełożeni pracowników odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia dostępu do danych osobowych.
38. Administrator Bezpieczeństwa Informacji w oparciu o informacje, o których mowa w ust. 3 powinien podjąć działania, których celem jest uniemożliwienie tym osobom dostępu do danych osobowych i wyrejestrować z ewidencji, o której mowa w ust. 1
39. Elektroniczne nośniki informacji, na których gromadzone są wykazy zawierające ewidencję osób upoważnionych do przetwarzania danych osobowych powinny być przechowywane w szafie zamykanej, do której ma dostęp Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.
40. Wzór karty z ewidencji stanowi **załącznik nr 3** niniejszej Polityki.

§ 16

Dostęp zdalny

41. Zastosowane przez Zespół Szkół rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność przetwarzanych danych osobowych oraz ochronę kryptograficzną wobec danych służących do uwierzytelniania przesyłanych publicznymi łączami telekomunikacyjnymi.
42. Nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe realizowane jest przez Administratora Systemu po spełnieniu wymagań określonych w ust. 1 oraz po uzyskaniu akceptacji Administratora Bezpieczeństwa Informacji.
43. Dostęp zdalny do danych osobowych przetwarzanych przez Zespół Szkół, możliwy jest wyłącznie dla tych użytkowników zewnętrznych, którzy prowadzą swoje prace na rzecz Zespołu Szkół , na podstawie obowiązującej umowy oraz po spełnieniu wymagań określonych w §21 niniejszej Polityki.
44. Dostęp do systemów informatycznych dla użytkowników zewnętrznych powinien być monitorowany pod kątem bezpieczeństwa przez Administratorów Systemu w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

§ 17

Rejestracja zbiorów danych osobowych

45. Upoważnieni pracownicy są zobowiązani do wnioskowania Administratorowi Bezpieczeństwa Informacji zamiaru utworzenia nowego zbioru danych osobowych wraz ze wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.
46. Administrator Bezpieczeństwa Informacji weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem obowiązku zgłoszenia zasobu, jako zbioru danych do rejestracji w GIODO.
47. W sytuacji, jeżeli rejestracja nowopowstałego zbioru danych osobowych jest ustawowo wymagana, Administrator Bezpieczeństwa Informacji przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO .
48. Administrator Bezpieczeństwa Informacji sprawdza opisane zgłoszeniu rejestracyjnym warunki techniczne i organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Dyrekcji o podniesienie poziomu tych zabezpieczeń.

49. Przygotowany przez Administratora Bezpieczeństwa Informacji projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przedstawiany dyrektorowi albo upoważnionemu członkowi Dyrekcji do podpisu.
50. Administrator Bezpieczeństwa Informacji uzupełnia Politykę, dokumenty z nią powiązane oraz pozostałe dokumenty obowiązujące w Spółce w zakresie ochrony danych osobowych o informacje na temat nowego zbioru.

§ 18

Aktualizacja zbiorów danych osobowych

51. Tryb określony w § 18 stosuje się również przy aktualizacji lub usunięciu wad zgłoszenia zbioru danych osobowych do rejestracji GIODO.
52. Administrator Bezpieczeństwa Informacji przygotowuje wniosek aktualizacyjny zarejestrowanego zbioru danych osobowych w terminie 30 dni od dnia dokonania zmiany w zbiorze.
53. Wniosek aktualizacyjny zarejestrowanego zbioru danych osobowych jest przedstawiany do akceptacji i podpisu dyrektorowi albo upoważnionemu członkowi Dyrekcji. Po podpisaniu przedmiotowe pismo jest wysyłane przez Administratora Bezpieczeństwa Informacji do GIODO.

§ 19

Udostępnianie danych osobowych

54. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, osobom upoważnionym do przetwarzania danych oraz osobom, których dotyczą.
55. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
56. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
57. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Administrator Bezpieczeństwa Informacji.
58. Odpowiedź na wniosek o udostępnienie danych osobowych jest podpisywana przez Dyrektora lub upoważnioną osobę z Dyrekcji.
59. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru, np. w następujący sposób:
    1) Listem poleconym za pokwitowaniem odbioru.
    2) Teletransmisji danych zgodnie z zasadami wymiany informacji opisanymi w § 13 niniejszej Polityki.
    3) Innym bezpiecznym, określonym wymogiem prawnym lub umową.
60. Informacja o udostępnieniu danych osobowych podlega odnotowaniu jeśli dane osobowe udostępniane są ze zbioru danych osobowych. W takim przypadku, odnotowaniu podlega informacja o zakresie danych podlegających udostępnieniu, dacie udostępnienia odbiorcy, celu udostępnienia oraz danych osób, które ze strony Zespołu Szkół udostępniły dane osobowe. Nie dotyczy to sytuacji, gdy przepisy prawa zezwalają na zbieranie danych osobowych bez konieczności ujawniania adresata danych.

§ 20

Powierzanie przetwarzania danych osobowych

61. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Zespołem Szkół mają dostęp do danych osobowych.
62. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 31 Ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych, pomiędzy Zespołem Szkół, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych.
63. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:
    1) Cel i zakres przetwarzania danych osobowych.
    2) Obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych.
    3) Konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy (z punktu widzenia ochrony danych osobowych).
    4) Wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.
64. Zalecane jest aby w umowach powierzenia przetwarzania danych osobowych oraz w umowach, na podstawie których dochodzi do wymiany informacji uwzględnić następujące elementy:
    1) Definicję informacji, która ma być chroniona.
    2) Spodziewany czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy.
    3) Wymagane działania w momencie zakończenia umowy.
    4) Odpowiedzialność i działania sygnatariuszy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji.
    5) Własność informacji, tajemnic przemysłowych i własności intelektualnej oraz jak odnosi się to do ochrony danych osobowych.
    6) Prawa do audytu i monitorowania działań związanych z ochroną danych osobowych.
    7) Proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych.
    8) Zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy.
    9) Działania podejmowane w przypadku naruszenia warunków umowy.
65. Projekt umowy powierzenia przetwarzania danych osobowych innemu podmiotowi przygotowuje Administrator Bezpieczeństwa Informacji.

§ 21

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

66. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.

67. Przed przystąpieniem do pracy pracownicy zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
68. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:
    1) Nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują.
    2) Nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu.
    3) Niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych.
    4) Nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu).
    5) Udostępnienie osobom nieupoważnionym danych osobowych lub ich części.
    6) Inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy.
    7) Wydarzenia losowe, obniżające poziom ochrony systemu (np. zalanie lub pożar).
    8) Kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).
69. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.
70. Do czasu przybycia Administratora Bezpieczeństwa Informacji, zgłaszający:
    1) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów.
    2) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym.
    3) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
    4) Wykonuje polecenia Administratora Bezpieczeństwa Informacji.
71. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji, po przybyciu na miejsce:
    1) Ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu.
    2) Wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem.
    3) Podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
72. Administrator Bezpieczeństwa Informacji sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:
    1) Dacie i godzinie powiadomienia.
    2) Godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane.

3) Sytuacji, jaką zastał.

4) Podjętych działaniach i ich uzasadnieniu.

5) Stanie systemu po podjęciu działań naprawczych.

6) Wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.

73. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji.

74. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Zespole Szkół dyscypliny pracy, Administrator Bezpieczeństwa Informacji wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

75. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

§ 22

Wykaz zbiorów danych osobowych

76. Zespół Szkół jest administratorem danych osobowych wymienionych w **załączniku nr 4** niniejszej Polityki.

77. Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń przetwarzania danych osobowych.

78. Administrator Bezpieczeństwa Informacji w oparciu o informacje uzyskane od pracowników, prowadzi wykaz systemów i aplikacji zastosowanych do przetwarzania danych osobowych.

§ 23

Opis struktury zbiorów danych osobowych

79. Opis struktury zbiorów danych osobowych zawiera **załącznik nr 4** niniejszej Polityki.

80. Wskazane w załączniku nr 4 zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach.

81. Aktualny opis struktury ww. zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi powinien być prowadzony przez Administratora Bezpieczeństwa Informacji w oparciu o informacje uzyskane od Administratorów Systemu.

§ 24

Sposób przepływu danych pomiędzy poszczególnymi systemami

82. Administrator Bezpieczeństwa Informacji, w oparciu o informacje uzyskane od pracowników, prowadzi dokumentację systemów informatycznych zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami w których te dane są przetwarzane. W **załączniku nr 5** opisano przepływ danych osobowych pomiędzy poszczególnymi systemami.

§ 25

Zasady ochrony danych osobowych w zbiorach nieinformatycznych

83. Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
84. Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
85. Na czas nie użytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.
86. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
87. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji.

§ 26

Postanowienia końcowe

88. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
89. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.

Załącznik nr 1 Wzór oświadczenia pracownika dotyczącego ochrony danych osobowych

…….
(data)

……..
(imię i nazwisko pracownika)

Oświadczenie pracownika

zatrudnionego przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez Zespół Szkół w Radzyniu Chełmińskim

Obowiązki pracownika

Pracownik dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

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

Odpowiedzialność pracownika

Za niedopełnienie obowiązków wynikających z niniejszego oświadczenia pracownik ponosi odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych a także Ustawy Karta Nauczyciela, jeżeli pracownik jest nauczycielem.

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

Potwierdzam odbiór 1 egz. oświadczenia..

…….. pracownik

…….. pracodawca

Załącznik nr 2 Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j.Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
– udziela się Panu/Pani*:

.....
(imię i nazwisko pracownika)

.....
(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych, których Administratorem Danych jest Zespół Szkół.

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych na nośnikach papierowych i w systemach informatycznych wyłącznie w zakresie wynikającym z Pana/Pani* zadań oraz poleceń przełożonego.

Upoważnienie traci ważność z chwilą ustania stosunku pracy.

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

---

* niepotrzebne skreślić

Załącznik nr 3 Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych

l.p.	Imię	Nazwisko	Stanowisko	Zakres upoważnienia	Identyfikator/nazwa systemu	Data nadania uprawnień	Data odebrania uprawnień
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							

Załącznik nr 4 Wykaz zbiorów danych osobowych oraz opis struktury zbiorów danych osobowych

1. Wykaz zbiorów danych osobowych

1. Zbiór danych kadrowych (nauczyciele i inni pracownicy),
2. Kandydaci do pracy,
3. Ewidencja dzieci i uczniów (obecnych i byłych) i związane z nimi dane rodziców,
4. Zbiór danych uczniów z okręgu szkoły realizujących obowiązek szkolny w innych szkołach,
5. Zbiór danych dzieci realizujących obowiązek rocznego przygotowania przedszkolnego w innych przedszkolach,
6. Zbiór uczniów, którym przyznawane są stypendia i wyprawka szkolna,
7. Zbiór uczniów objętych pomocą psychologiczno – pedagogiczną,
8. Zamówienia publiczne,
9. Ewidencja osób ubiegających się o uzyskanie informacji publicznej,
10. Rejestr skarg i wniosków,
11. Rejestr korespondencji,
12. Zbiór danych prowadzonych na potrzeby sprawdzianu kompetencji w klasie szóstej SP i klas trzecich Gimnazjum,
13. Zbiór danych prowadzony w ramach systemu informacji oświatowej.

2. Opis struktury zbiorów danych osobowych

1) Nazwa zbioru: Zbiór danych kadrowych

Kategoria osób: nauczyciele i inni pracownicy

Dane identyfikujące: imię i nazwisko, adres, dane kontaktowe (np. nr tel. stacjonarnego lub komórkowego), data urodzenia, rysopis (np. zdjęcie), nr NIP, nr PESEL, seria i nr dowodu osobistego oraz stosunek do służby wojskowej.
Dane kontaktowe: imię i nazwisko, miejsce pracy, funkcja lub stanowisko, (ewentualnie nr certyfikatu) podpis, służbowy adres e-mail
Dane dotyczące wykształcenia oraz ukończonych kursów: poziom wykształcenia, data ukończenia szkoły, nazwa ukończonej szkoły w przypadku szkoły wyższej, typ ukończonej szkoły, profil, stopień (tytuł naukowo – zawodowy), specjalizacja, ukończone studia podyplomowe, ukończone kursy, ważniejsze szkolenia, posiadane uprawnienia, kwalifikacje, inne umiejętności, znajomość systemów informatycznych, stopień znajomości języków obcych,
Dane służące do reprezentacji: imię i nazwisko, miejsce pracy, funkcja lub stanowisko, (ewentualnie nr certyfikatu) podpis, służbowy adres e-mail, seria i nr dowodu osobistego
Dane dotyczące rodziny: stan cywilny, nazwisko panieńskie matki, imiona rodziców, imię i nazwisko oraz data urodzenia współmałżonka, imię i nazwisko, data urodzenia dziecka lub dzieci pracownika, imię i nazwisko, adres oraz nr telefonu osoby, która należy poinformować w razie wypadku pracownika
Dane dotyczące przebiegu zatrudnienia: adres do korespondencji, nazwisko panieńskie, obywatelstwo, przebieg kariery, czas pracy, dane dotyczące zdolności do pracy, informacje o nr rachunku bankowego, wysokość wynagrodzenia, nagrody, premie, kwoty udzielonych pożyczek, informacje o zatrudnieniu u innego pracodawcy

Dane dotyczące ubezpieczenia społecznego i zdrowotnego: informacje o oddziale Narodowego Funduszu Zdrowia
Dane dotyczące karalności: oświadczenie o ukaraniu sądowym

2) Nazwa zbioru: kandydaci do pracy

Kategoria osób: kandydaci do pracy

Dane identyfikujące: imię i nazwisko, podpis, adres e-mail, nr telefonu.
Dane dotyczące wykształcenia oraz ukończonych kursów: poziom wykształcenia, data ukończenia szkoły, nazwa ukończonej szkoły w przypadku szkoły wyższej, typ ukończonej szkoły, profil, stopień (tytuł naukowo – zawodowy), specjalizacja, ukończone studia podyplomowe, ukończone kursy, ważniejsze szkolenia, posiadane uprawnienia, kwalifikacje, inne umiejętności, znajomość systemów informatycznych, stopień znajomości języków obcych,
Dane dotyczące przebiegu zatrudnienia: adres do korespondencji, nazwisko panieńskie, obywatelstwo, przebieg kariery, czas pracy, dane dotyczące zdolności do pracy, informacje o zatrudnieniu u innego pracodawcy
Dane dotyczące karalności: oświadczenie o ukaraniu sądowym

3) Nazwa zbioru: ewidencja dzieci i uczniów (obecnych i byłych) i związane z nimi dane rodziców (prawnych opiekunów)

Dane identyfikujące: imię i nazwisko, adres, data i miejsce urodzenia, nr PESEL, imiona i nazwiska rodziców (prawnych opiekunów), miejsce zamieszkania rodziców (prawnych opiekunów)
Dane kontaktowe: imię i nazwisko rodziców (prawnych opiekunów) podpis, nr telefonu, adres e-mail

4) Nazwa zbioru: Zbiór danych uczniów z okręgu szkoły realizujących obowiązek szkolny w innych szkołach,

Dane identyfikujące: imię i nazwisko, adres, data i miejsce urodzenia, nr PESEL, imiona i nazwiska rodziców (prawnych opiekunów), miejsce zamieszkania rodziców (prawnych opiekunów), nazwa szkoły lub placówki, w której uczeń realizuje obowiązek szkolny,

5) Nazwa zbioru: Zbiór danych dzieci realizujących obowiązek rocznego przygotowania przedszkolnego w innych przedszkolach

Dane identyfikujące: imię i nazwisko, adres, data i miejsce urodzenia, nr PESEL, imiona i nazwiska rodziców (prawnych opiekunów), miejsce zamieszkania rodziców (prawnych opiekunów), nazwa przedszkola lub placówki, w której dziecko realizuje obowiązek rocznego przygotowania przedszkolnego,

6) Nazwa zbioru: Zbiór uczniów, którym przyznawane są stypendia i wyprawka szkolna

Dane identyfikujące: imię i nazwisko, klasa,

Dane dotyczące stypendium: nazwa stypendium, fundator stypendium, kwota stypendium, dochód w rodzinie i sytuacja rodzinna (tylko w sytuacji, gdy przyznanie stypendium wymaga takich informacji)

7) Nazwa zbioru: Zbiór uczniów objętych pomocą psychologiczno – pedagogiczną,

Dane identyfikujące: imię i nazwisko, klasa, adres, data i miejsce urodzenia

Dane dotyczące problemów dziecka lub ucznia: stopień niepełnosprawności, form nauczania,

stan zdrowia, choroby, dysfunkcje, problemy edukacyjne, szczególna sytuacja losowa, zastosowane formy pomocy psychologiczno – pedagogicznej,

8) Nazwa zbioru: Zamówienia publiczne,

   Dane identyfikujące:

9) Ewidencja osób ubiegających się o uzyskanie informacji publicznej,

   Dane identyfikujące; imię nazwisko, adres, nr dowodu osobistego, nr PESEL

10) Nazwa zbioru: Rejestr skarg i wniosków,

    Dane identyfikujące:

11) Nazwa zbioru: Zbiór danych prowadzonych na potrzeby sprawdzianu kompetencji w klasie szóstej SP i klas trzecich Gimnazjum,

    Dane identyfikujące: imię i nazwisko, klasa, adres, data i miejsce urodzenia

    Dane uzupełniające: nazwa dysfunkcji, rodzaj i stopień niepełnosprawności, forma dostosowania warunków sprawdzianu, rodzaj testu, wyniki sprawdzianu lub egzaminu

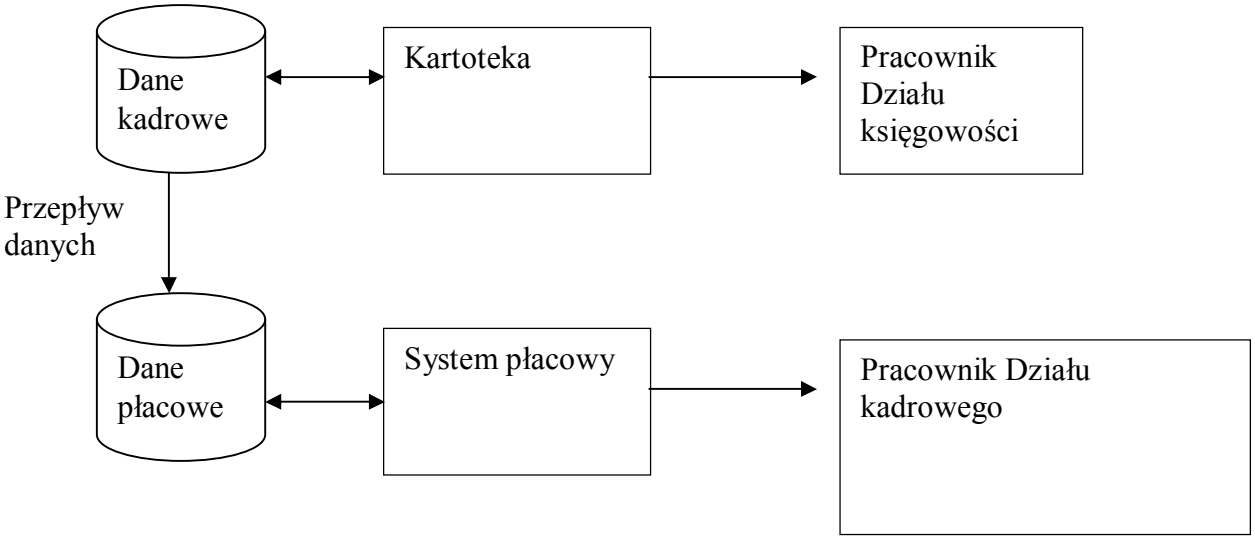
12) Nazwa zbioru: Zbiór danych prowadzony w ramach systemu informacji oświatowej

    Dane identyfikujące nauczyciela: nr PESEL, płeć, rok urodzenia,

    Dane dotyczące zatrudnienia: stopień awansu zawodowego, wykształcenie, podstawa świadczenia stosunku pracy, tygodniowy wymiar zatrudnienia, ilość godzin ponadwymiarowych, staż pracy ogólny i pedagogiczny, stanowisko, wynagrodzenie, obowiązki, nieobecność, kwalifikacje, dodatkowe uprawnienia zawodowe w dziedzinie kultury fizycznej i sportu, ukończone formy kształcenia i doskonalenia zawodowego, wysokość dodatku wiejskiego i mieszkaniowego

Załącznik nr 5 Opis przepływu danych osobowych

1 Przepływ danych kadrowych



Załącznik nr 6 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Przetwarzanie danych osobowych przez Zespół Szkół w Radzyniu Chełmińskim przy ul. Sady 14, i następuje we wszystkich budynkach Zespołu Szkół w Radzyniu Chełmińskim i Rywałdzie w następujących pomieszczeniach:

1. Stacje robocze, na których przetwarzane są dane osobowe znajdują się w pomieszczeniach o numerach: gabinet dyrektora - 88 , gabinety wicedyrektorów - 88,54,101 sekretariat - nr 87, zaplecze wicedyrektora ds. gimnazjum – 105, biuro głównej księgowej - 94, biuro specjalisty ds. zatrudnienia i płac - 92, biuro kierownika gospodarczego - 91, biuro dietetyczki - 90, gabinety pedagogów szkolnych – 13, 70, gabinet logopedy - 64, pokoje nauczycielskie – 1, 20, 71,… , biblioteka - 99, świetlica - 97, sale lekcyjne – 9, 12, 14, 15, 16, 17, 21, 23, 24, 27, 30, 31, 34, 35, 40, 46, 61, 62, 63, 68, 69, 72, 73, 74, 78, 79, 80, 81, 100, 101, 102, 107
2. Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe zlokalizowane są w pomieszczeniach : gabinet dyrektora - 88 , gabinety wicedyrektorów - 54, 88, 104, sekretariat – nr 105, zaplecze wicedyrektora ds. gimnazjum – 105, biuro głównej księgowej - 94, biuro specjalisty ds. zatrudnienia i płac - 92,
3. Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zlokalizowane są w pomieszczeniach: gabinet dyrektora - 88 , gabinety wicedyrektorów - 54, 88, 104, sekretariat - nr 105, biuro głównej księgowej - 94, biuro specjalisty ds. zatrudnienia i płac - 92, biuro kierownika gospodarczego - 91, biuro dietetyczki - 90, gabinety pedagogów szkolnych 13, 77
4. Kartoteki papierowe zawierające zbiory nieinformatyczne umiejscowione są w pomieszczeniach gabinet dyrektora - 88 , gabinety wicedyrektorów - 54, 88, 104, sekretariat - nr 105, zaplecze wicedyrektora ds. gimnazjum – 105, biuro głównej księgowej - 94, biuro specjalisty ds. zatrudnienia i płac - 92, biuro kierownika gospodarczego - 91, biuro dietetyczki - 90, gabinety pedagogów szkolnych – 13, 70, gabinet logopedy - 64, pokoje nauczycielskie 1, 20, 71,