POLITYKA BEZPIECZEŃSTWA
W ZAKRESIE OCHRONY DANYCH OSOBOWYCH
W PRZEDSZKOLU PUBLICZNYM NR 5 IM. KUBUSIA PUCHATKA
W RADZIKOWIE

Podstawa prawna :
- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity Dz. U. z 2002 r. nr 101, poz. 926)
- Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Rozdział I
Postanowienia ogólne
§ 1

Polityka bezpieczeństwa określa środki techniczne i organizacyjne zastosowane przez administratora danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.

§ 2

Ilekroć w Polityce jest mowa o:
1) zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
2) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbierania, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
3) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych;
4) kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierających dane osobowe;
5) Administratorze Danych – rozumie się przez to Przedszkole Publiczne Nr 5 im. Kubusia Puchatka w Radzikowie reprezentowane przez Dyrektora Przedszkola;
6) Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych. Nadzór dotyczy przede wszystkim stosowanych środków technicznych

i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Przeprowadza on także kontrole w zakresie określonym regulacjami wewnętrznymi obowiązującymi u Administratora Danych;
7) osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację – rozumie się przez to informatyka odpowiedzialnego za powyższe zadania wyznaczonego przez Administratora Danych, zwanego dalej „Informatykiem";
8) użytkowniku – rozumie się osobę upoważnioną przez Administratora Danych do przetwarzania danych osobowych w systemie informatycznym oraz w kartotekach;
9) pomieszczeniach – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworząc obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

§ 3

1. Procedura ochrony danych osobowych jest zestawem reguł i praw regulujących sposób zarządzania, przetwarzania, przechowywania danych osobowych ze zbiorów w Przedszkolu Publicznym Nr 5 im. Kubusia Puchatka w Radzikowie.

§ 4

2. Celem procedury ochrony danych jest zapewnienie maksymalnego poziomu bezpieczeństwa procesu przetwarzania danych osobowych i ochrony przed nieuprawnionym dostępem i ich modyfikacją, utratą poufności przy zachowaniu ich integralności oraz wprowadzanie i realizację działań statutowych przy wykorzystaniu środków technicznych.
3. Procedura ochrony danych osobowych obowiązuje wszystkich pracowników Przedszkola Publicznego Nr 5 im. Kubusia Puchatka w Radzikowie.

§ 5

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochrony. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowanie zabezpieczania mają służyć osiągnięciu poniższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom.
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe zostały zmienione lub zniszczone w sposób nieautoryzowany.
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.
   4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność manipulacji, zarówno zamierzonej jak i przypadkowej.
   5) zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania Przedszkola Publicznego Nr 5 im. Kubusia Puchatka w Radzikowie i realizowania zadań określonych w odrębnych przepisach.

W związku z tym przedszkole może przetwarzać tylko takie informacje o pracownikach, które mają bezpośredni i jednoznaczny związek ze stosunkiem pracy oraz tylko takie informacje o dziecku, które związane są z procesem wychowawczym, dydaktycznym, opiekuńczym oraz ochroną zdrowia podczas pobytu w placówce.

§ 6

Realizację zamierzeń określonych w § 5 powinny zagwarantować następujące założenia:

1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych.
2) Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych.
3) Upoważnienie użytkowników do przetwarzania danych osobowych oraz przypisanie użytkownikom określonych atrybutów umożliwiających wykonywanie ustalonych operacji na różnych poziomach zbiorów danych osobowych – stosowanie do indywidualnego zakresu upoważnienie, zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.
4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń.
5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.

Rozdział II

Opis zdarzeń naruszających ochronę danych osobowych

§ 7

Zdarzeniami naruszającymi ochronę danych osobowych bądź stwarzającymi podejrzenie naruszenia zabezpieczeń danych mogą być następujące przypadki:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasobach systemu jak np. : pożar, zalanie pomieszczeń, katastrofa budowlana itp.
2) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na celowe działanie w kierunku naruszenia ochrony danych, a także właściwie działania serwisu.
3) Komunikaty alarmujące o próbie naruszenia zabezpieczenia systemu, które zapewnia ochronę danych bądź komunikatu o podobnym znaczeniu.
4) Odstępstwa od prawidłowego stanu danych wskazujące na niewłaściwe działanie systemu i pożądaną jego modyfikację.
5) Naruszenie lub próba naruszenia integralności systemu bazy danych w tym systemie.
6) Modyfikacja lub próba modyfikacji danych oraz zmiana w strukturze danych dokonana bez odpowiedniego upoważnienia.
7) Stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie.
8) Ujawnienie danych osobowych lub objętych tajemnicą procedur ochrony danych osobowych osobom nieupoważnionym , bądź innych elementów systemu zabezpieczeń.
9) Funkcjonowanie sieci komputerowej lub praca systemu wykazuje nieprzypadkowe odstępstwo od prawidłowego rytmu pracy wskazujące na zaniechanie lub przełamanie ochrony danych w sposób niedozwolony lub przez osobę nieupoważnioną.
10) Ujawnienie istnienia nieautoryzowanych kont dostępu do danych objętych ochroną.

11) Zniszczenie lub podmiana nośnika z danymi osobowymi bądź skasowanie lub skopiowanie danych osobowych w sposób niedozwolony lub przez osobę nieupoważnioną.
12) Rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji np. nie wylogowanie się z systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niewykonanie w określonym terminie kopii bezpieczeństwa, praca na danych osobowych w celach prywatnych itp.
13) Stwierdzenie nieprawidłowości w zakresie nie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały) na nośnikach tradycyjnych tj. na papierze, folii, zdjęciach, dyskietkach w formie zabezpieczonej itp.

Rozdział III

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 8

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.
3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych
4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemie informatycznym, jak i w kartotekach.

§ 9

1. 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 .

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia danych.

§ 10

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji po przybyciu na miejsce:

1) Ocenia zaistniałą sytuacje, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu.
2) Wysłuchuje relacji osoby, która dokonała powiadomienia.
3) Podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
   W uzasadnionych przypadkach niezwłocznie powiadamia Administratora danych.

§ 11

1. Administrator Bezpieczeństwa Informacji sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:

1) Dacie godzinie powiadomienia.
2) Godzinie pojawienia się w pomieszczeniach , w których przetwarzane są dane.
3) Sytuacji którą zastał.
4) Podjętych działaniach i ich uzasadnieniu

2. Kopia raportu przekazywana jest bezzwłocznie Administratorowi Danych.

§ 12

1. Administrator Bezpieczeństwa Informacji podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu :

1) W miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu.
2) Relacjonuje Administratorowi Danych przedsięwzięte czynności.
3) O ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób dopuszczonych do przetwarzania danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, Administrator Bezpieczeństwa Informacji wnioskuje do Administratora Danych o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy / sprawców.

§ 13

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

§ 14

1. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
2. W sytuacji o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub której zginął sprzęt oraz powiadamia Administratora Danych.

§ 15

Osoba dopuszczona do przetwarzania danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki ponosi odpowiedzialność przewidzianą w odrębnych przepisach prawa.

Rozdział IV

Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

§ 16

Dla skutecznej realizacji Polityki Administrator Danych Osobowych zapewnia:

1) Odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne.
2) Szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony.
3) Monitorowanie zastosowanych środków ochrony.

§ 17

1. Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, którym w Przedszkolu Publicznym nr 5 w Radzikowie jest indendent - wzór upoważnienia w **załącznik Nr 1**.
2. Administrator Bezpieczeństwa Informacji realizuje zadania z zakresu ochrony danych, a w szczególności:

1) Ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych w przedszkolu.
2) Dokonuje okresowej kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzeganiem zasad postępowania w przypadku naruszenia ochrony danych osobowych.
3) Prowadzi rejestr dokonanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonanie.
4) Z kontroli sporządza protokoły, które przechowuje Administrator Danych Osobowych.
5) Podejmuje stosowne działania zgodnie z niniejszą Polityką Bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpiecza dane znajdujących się w systemie informatycznym.

6) Niezwłocznie informuje Administratora danych Osobowych lub osobę przez niego upoważnioną w przypadku naruszenia przepisów ustawy o ochronie danych osobowych.
7) Przeprowadza szkolenia dla pracowników z ochrony danych osobowych.

3. Zarządzanie bezpieczeństwem systemów służących do przetwarzania danych osobowych jest procesem ciągłym, realizowanym przy współdziałaniu osób upoważnionych do przetwarzania danych z Administratorem Danych Osobowych i Administratorem Bezpieczeństwa Informacji.

§ 18

Osoby upoważnione przez Administratora Danych Osobowych do przetwarzania danych osobowych zobowiązane są do :

1) Ścisłego przestrzegania zakresu udzielonego upoważnienia.
2) Zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania.
3) Przetwarzania danych osobowych wyłącznie przy użyciu przydzielonego im komputera zabezpieczonego hasłem przed nieupoważnionym użyciem.
4) Zgłaszania do Administratora Danych Osobowych przypadków naruszenia bezpieczeństwa danych lub przypadków niewłaściwego działania systemu
5) Przestrzegania obowiązujących w tym zakresie przepisów, zarządzeń, instrukcji.

Rozdział V

Środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, integralności i przetwarzania danych

§ 19

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:
1) Przetwarzanie danych osobowych w przedszkolu może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
2) Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.
3) Unieważnienie upoważnienia następuje na piśmie.
4) Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się za zgodą Administratora Danych.
5) Każdy upoważniony do przetwarzania danych oświadcza pisemnie fakt zapoznania się z niniejszą dokumentacją -**załącznik nr 2.**
6) Obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
7) Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora Danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

8) Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
9) Klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu.
10) Klucze wydawane są wyłącznie osobom upoważnionym.
11) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
12) Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna, usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w zamykanych szafach .
13) Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych.
14) Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych.
15) W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych osobowych jest zabronione.
16) **Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone**.

2. Środki techniczne ochrony danych osobowych.

1) Zbiory danych osobowych należy przechowywać w przeznaczonych do tego szafach, zamykanych na klucz, do których dostęp mają tylko osoby upoważnione.
2) Składowanie zbiorów danych osobowych (w tym wymiennych i nośników kopii zapasowych) odbywa się w odpowiednio zabezpieczonych szafach.
3) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4) Zastosowano środki ochrony przed szkodliwym oprogramowaniem.
5) Użyto system Firewall do ochrony dostępu do sieci komputerowej.
6) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
7) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
8) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
9) Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa **Instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych.

Rozdział VI
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
§ 20

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, w pomieszczeniach

Administratora Danych i są to:
1) Gabinet dyrektora przedszkola
2) Biuro- pokój Intendenta
3) Pokój nauczycielski

2. Pomieszczania znajdują się w Przedszkolu Publicznym Nr 5 im. Kubusia Puchatka w Radzikowie.

Rozdział VII

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych

§ 21

1. Dane osobowe przetwarzane są w formie papierowej i elektronicznej przy użyciu następujących programów: SIO, Vulcan, MS Office.
2. Zbiory danych przetwarzane w postaci tradycyjnej są przechowywane w szafach lub pomieszczeniach zamykanych na klucz.
3. Przebywanie osób trzecich w pomieszczeniach, gdzie są przetwarzane dane osobowe dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych lub w obecności przełożonego.
4. Szczegółowy wykaz zbiorów danych osobowych, ich struktura ze wskazaniem programów zastosowanych do ich przetwarzania zawiera **załącznik nr 3**

Rozdział VIII
Gromadzenie, przepływ zbiorów danych osobowych

§ 22

1. Dane osobowe pozyskiwane są z danych źródeł. Dane te gromadzone są w systemach informatycznych i na nośnikach papierowych.

2. W Przedszkolu Publicznym Nr 5 im. Kubusia Puchatka dane osobowe przetwarzane są w zbiorach danych przy zastosowaniu systemów oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, wykazów.

3. Zawartość pól informacyjnych występujących w systemach zastosowanych w celu przetwarzania danych osobowych musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora Danych Osobowych do przetwarzania danych osobowych.

§ 23

1. W uzasadnionych sytuacjach jest możliwe przesłanie danych osobowych do Urzędu Miejskiego w Błoniu, Kuratorium Oświaty, Poradni Psychologiczno - Pedagogicznej w Błoniu, Sądu, Policji, OPS w Błoniu.

2. Udostępnienie danych osobowych osobom, podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa na ich pisemny umotywowany wniosek.

3. Fakt udostępnienia danych osobowych odnotowany jest w dzienniku korespondencji.

ROZDZIAŁ IX
Postanowienia końcowe
§ 24

Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

§ 25

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obwiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

……
(podpis Administratora Danych)

Załącznik Nr 1 do Polityki Bezpieczeństwa

……
(miejscowość, data)

UPOWAŻNIENIE

Na podstawie (Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r.) (tekst jednolity Dz. U. z 2002 r. nr 101, poz. 926) , wyznaczam **……..** Administratorem Bezpieczeństwa Informacji w Przedszkolu Publicznym Nr 5 im. Kubusia Puchatka w Radzikowie.
Zobowiązuję Panią do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

…….
(podpis Administratora Danych)

Załącznik Nr 2 do Polityki Bezpieczeństwa

_____ _____

(imię i nazwisko) (miejscowość, data)

OŚWIADCZENIE

Oświadczam, iż zostałam*/zostałem* zaznajomiona*/zaznajomiony* z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Polityką bezpieczeństwa danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Jednocześnie zobowiązuję się do ich przestrzegania.

(podpis osoby składającej oświadczenie)

* niepotrzebne skreślić

Załącznik Nr 3 do Polityki Bezpieczeństwa

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

l.p.	Nazwa zbioru	Struktura zbioru	Program
1.	Dokumentacja dzieci przedszkolnych	Nazwisko, imię, data i miejsce urodzenia, adres zamieszkania lub pobytu, pesel, oraz nazwisko, imię, adres zamieszkania, telefon rodziców, email rodziców	SIO
2.	Umowa na pobyt dziecka w przedszkolu	Nazwisko, imię, adres zamieszkania, PESEL, dowód osobisty rodziców	
3.	Dziennik zajęć przedszkola	Nazwisko, imię, data i miejsce urodzenia, adres zamieszkania lub pobytu dziecka, oraz nazwiska, imiona, adresy zamieszkania, telefony email rodziców	
4.	Arkusz obserwacji dziecka	Nazwisko, imię, informacje dot. rozwoju dziecka	
5.	Dokumentacja wypadków dzieci	Nazwisko, imiona, adres zamieszkania lub pobytu, stan zdrowia dziecka	
6.	Dokumentacja kadrowo-płacowa	Nazwisko, imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, wykształcenie, przebieg dotychczasowego zatrudnienia, wynagrodzenie pracownika, imiona rodziców	Vulcan

7.	Awans Zawodowy	Nazwisko, imiona,, data urodzenia, adres zam. przebieg zatrudnienia, wykształcenie	
8.	Dokumentacja wypadków pracowników	Nazwisko, imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, stan zdrowia	
9.	Zakładowy Fundusz Świadczeń Socjalnych	Nazwisko, imiona, adres zamieszkania lub pobytu, stan zdrowia, wynagrodzenie	
10.	Fundusz zdrowotny dla nauczycieli	Nazwisko, imiona, adres zamieszkania lub pobytu, stan zdrowia	
11.	Umowy zlecenia	Nazwisko, imiona, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu	
12.	Rekrutacja	Nazwisko, imię, data i miejsce urodzenia, adres zamieszkania lub pobytu, pesel, oraz nazwisko, imię, adres zamieszkania, telefon rodziców, email rodziców	
13.	Upoważnienia do odbioru	Nazwisko, imię dziecka, nazwisko, imię osoby upoważnionej do odbioru, adres zamieszkania, seria i nr dowodu osobistego	
14.	Rejestracja korespondencji, skarg i wniosków	Nazwisko, imię, adres zamieszkania lub pobytu, telefon	
15.	Konkursy	Nazwisko, imię dziecka	
16.	Praktyki	Nazwisko, imię, adres zamieszkania, telefon	