POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH

Administrator danych osobowych reprezentowany przez:

Dyrektora Przedszkola

Jolantę Laskowską

dnia 25.05.2018r. w jednostce organizacyjnej o nazwie

MIEJSKIE PRZEDSZKOLE NR 4 W ZAMBROWIE

na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

WDRAŻA

dokument o nazwie **„Polityka bezpieczeństwa informacji i ochrony danych osobowych”**.

Rozdział I

Postanowienia ogólne

§ 1

Deklaracja i zastosowanie

1. Realizując obowiązki wynikające z przepisów dotyczących ochrony danych osobowych administrator danych dąży do spełnienia wymagań chroniących prywatność i godność personelu, uczniów przedszkola oraz ich rodziców.
2. Dokument - Polityka bezpieczeństwa w zakresie ochrony informacji i danych osobowych w Miejskim Przedszkolu nr 4 w Zambrowie, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia zgodności z prawem, rzetelności i przejrzystości przetwarzania danych,

gwarancji adekwatności danych oraz ich minimalizacji, zbierania w konkretnych, wyraźnych i prawnie uzasadnionych celach. Dokument jest jednym ze środków organizacyjnych wprowadzonych przez administratora danych, mającym na celu wykazanie rozliczalności – przestrzegania przepisów ujętych w art. 5 ust. 1 RODO. Polityka odnosi się do zbiorów przetwarzanych w sposób tradycyjny – manualny oraz za pomocą systemu informatycznego.

3. Pracownicy zobowiązani są przestrzegać zasad bezpieczeństwa danych określonych w polityce bezpieczeństwa, a także współpracować we wdrażaniu oraz doskonaleniu procedur ochrony informacji. Zgłaszają uwagi i opiniują zastosowane rozwiązania.
4. Celem opracowania Polityki Bezpieczeństwa Informacji jest określenie zasad ochrony danych osobowych przetwarzanych w Miejskim Przedszkolu Nr 4 w Zambrowie. Zasady określone w niniejszej Polityce mają zastosowanie do wszystkich osób upoważnionych przez administratora do przetwarzania danych osobowych, niezależnie od formy ich zatrudnienia. Utrzymanie bezpieczeństwa przetwarzanych przez przedszkole danych osobowych oraz informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności na wysokim poziomie.
5. Procedury i dokumenty związane z Polityką będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.
6. Niniejsza Polityka została opracowana w oparciu o standardy PN-ISO/IEC 27001:2014-12.

§ 2

Definicje

Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1. rozporządzeniu (RODO) – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
2. zbiorze danych – rozumie się przez to każdy uporządkowany zestaw danych osobowych dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

3. przetwarzaniu danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
4. systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
5. zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
6. usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
7. pseudonimizacji – przetworzenie danych osobowych, w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
8. zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą w formie oświadczenia bądź wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
9. bezpieczeństwie danych – rozumie się przez to zapewnienie poufności, integralności i dostępności informacji, a także takich właściwości jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
10. incydencie – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które zagrażają bezpieczeństwu informacji;
11. administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 4 pkt.7 RODO, decydujący o celach i środkach przetwarzania danych osobowych – rozumianym jako Miejskie Przedszkole nr 4 w Zambrowie, reprezentowane przez Dyrektora Przedszkola;

12. inspektorze ochrony danych – rozumie się przez to osobę powołaną przez administratora danych osobowych w celu nadzoru nad przestrzeganiem stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
13. podmiocie przetwarzającym – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
14. odbiorcy – oznacza osobę fizyczną bądź prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią.
15. jednostce – rozumie się przez to jednostkę organizacyjną – Miejskie Przedszkole Nr 4 w Zambrowie.

§ 3

Inspektor ochrony danych

1. Administrator danych osobowych w Miejskim Przedszkolu Nr 4 w Zambrowie wyznacza inspektora ochrony danych w celu nadzoru nad przestrzeganiem stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
2. Administrator danych osobowych jest zobowiązany zawiadomić o wyznaczeniu inspektora ochrony danych organ nadzorczy oraz opublikować jego dane kontaktowe.

§ 4

Odpowiedzialność

Za bezpieczeństwo danych osobowych odpowiedzialny jest właściciel – Miejskie Przedszkole nr 4 w Zambrowie, oraz każda osoba upoważniona przez Dyrektora Przedszkola do przetwarzania danych osobowych, niezależnie od formy zatrudnienia. Zgodnie z wymaganiami rozporządzenia – do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie nadane przez administratora danych osobowych. Administrator danych osobowych upoważniając osoby do przetwarzania danych osobowych zachowuje zasadę, że dostęp do danych osobowych będą miały tylko te osoby, którym jest to niezbędne do realizacji powierzonych zadań. Każda z osób upoważnionych do przetwarzania danych osobowych zostanie, przed dopuszczeniem do przetwarzania danych, przeszkolona z wymagań dotyczących ochrony danych osobowych oraz poinformowana o konsekwencjach prawnych jakie jej grożą za naruszenie tych zasad.

Reguły zatrudnienia pracownika przy przetwarzaniu danych, etap naboru oraz zakończenia stosunku pracy oraz ogólne zasady bezpieczeństwa osobowego zawarte są w załączniku nr 8 do niniejszej polityki.

Administrator danych osobowych postanawia, że do wydawania upoważnień do przetwarzania danych osobowych upełnomocniony zostaje inspektor ochrony danych, który czuwa również nad aktualnością przyznawanych upoważnień w związku ze zmianami kadrowymi. Wszystkie upoważnienia do przetwarzania danych znajdują się w *ewidencji osób upoważnionych do przetwarzania danych*, którą prowadzi inspektor ochrony danych – *załącznik nr 7*.

Osoby nieupoważnione do przetwarzania danych osobowych, mogą przebywać w obszarze przetwarzania oraz przechowywania danych osobowych podczas nieobecności osoby upoważnionej do przetwarzania wyłącznie za zgodą administratora danych osobowych podpisując oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami

§ 5
Zasady ochrony informacji

System zarządzania bezpieczeństwem informacji zgodny z wymaganiami niniejszej polityki opiera się na następujących niezaprzeczalnych zasadach ochrony informacji:

1. Zasada znajomości wymagań Polityki Bezpieczeństwa Informacji – każdy pracownik powinien zostać zapoznany z regułami oraz kompletnymi i aktualnymi procedurami ochrony informacji i podpisać stosowne oświadczenie o zapoznaniu się z zasadami obowiązującej polityki.
2. Zasada uprawnionego dostępu – każdy pracownik stosuje się do obowiązujących zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji.
3. Zasada przywilejów koniecznych – każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonania powierzonych mu zadań.
4. Zasada wiedzy koniecznej – każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
5. Zasada usług koniecznych – systemy świadczą tylko te usługi, które są konieczne do realizacji zadań statutowych przedszkola.
6. Zasada świadomości zbiorowej – wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie;

7. Zasada indywidualnej odpowiedzialności – za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
8. Zasada obecności koniecznej – prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione.
9. Zasada stałej gotowości – system jest przygotowany na wszelkie zagrożenia, niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
10. Zasada najsłabszego ogniwa – poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element. Elementy te są wyznaczane na podstawie analizy ryzyka.
11. Zasada kompletności – skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
12. Zasada ewolucji – każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
13. Zasada adekwatności – używane środki techniczne i organizacyjne winny być odpowiednie do sytuacji.
14. Zasada segregacji zadań – zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła samodzielnie decydować o funkcjonowaniu całego systemu.

§ 6

W celu zwiększenia efektywności ochrony informacji dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona informacji jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Cele i strategie bezpieczeństwa:

1. zgodność z prawem;
2. ochrona zasobów informacyjnych i innych aktywów;
3. uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań;
4. zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty;
5. zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa informacji wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

§ 7

Realizacje zamierzeń określonych w § 5 powinny zagwarantować następujące założenia:

1. wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania informacji oraz odpowiedzialność za ochronę danych
2. przeszkolenie pracowników w zakresie bezpieczeństwa i ochrony informacji
3. przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory)
4. podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń
5. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych
6. opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii
7. okresowe aktualizowanie Polityki Bezpieczeństwa Informacji
8. identyfikacja zagrożeń i analiza ryzyka.

§ 8

Zdarzenia naruszające ochronę danych

Zgodnie z art. 34 RODO Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Opis zdarzeń naruszających ochronę danych osobowych przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych oraz postępowania w przypadku naruszenia ochrony danych stanowi *załącznik nr 4* do niniejszej Polityki – *Zarządzenie ryzykiem utraty bezpieczeństwa danych.*

§ 9

Udostępnianie danych osobowych

1. Udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
2. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały ujawnione.
3. Podmiot występujący o ujawnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymywania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym

przypadku ujawnienie danych jest prawnie dopuszczalne i czy nie będzie stanowić ono naruszenia zasad ochrony danych osobowych. *(Motyw 31 RODO)*

4. Udostępnienie danych może nastąpić jedynie na podstawie pisemnego wniosku strony trzeciej. Wniosek musi zawierać co najmniej dane wnioskodawcy, dane Administratora danych (celem potwierdzenia właściwości skierowania wniosku o udostępnienie danych osobowych), podstawę prawną upoważniającą do pozyskania informacji, wskazanie przeznaczenia dla udostępnionych danych, zakres informacji.
5. Udostępnienie informacji może nastąpić jedynie za zgodą Administratora danych i powinno być odpowiednio udokumentowane.
6. Informacje o ujawnieniu danych osobowych należy zawrzeć w – *Rejestrze ujawnionych danych osobowych – stanowiący załącznik nr 5.*

§ 9
Podmiot przetwarzający

W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów zarządzania bezpieczeństwem ochrony danych niezbędne jest zawarcie umowy powierzenia przetwarzania danych osobowych i określenie w niej następujących wymagań bezpieczeństwa:

1. zakres i cel czynności oraz danych mających być przedmiotem zawartej umowy;
2. zakres odpowiedzialności w przypadku utraty bądź ujawnienia danych;
3. opis środków technicznych i organizacyjnych niezbędnych w celu zachowania bezpieczeństwa danych osobowych;
4. warunki dostępu do informacji – zobowiązanie do zachowania poufności osób uczestniczących w procesie przetwarzania;
5. wyznaczenie terminu obowiązywania umowy, uwzględniając bezterminowy obowiązek zachowania poufności;
6. wymaganych działań w momencie zakończenia umowy.

Inspektor ochrony danych prowadzi *Rejestr umów powierzenia przetwarzania danych osobowych,* stanowiący *załącznik nr 6 do niniejszej Polityki*.

§ 10
Grupy informacji podlegające ochronie

1. Grupa informacji dotycząca zadań statutowych:

a. dane osobowe uczniów;
b. dane osobowe dotyczące rodziców;
c. dane osobowe kandydata do przedszkola oraz jego rodziców
d. wnioski, zażalenia, skargi.

2. Grupa informacji dotycząca pracowników:
   a. dane osobowe pracowników;
   b. dane osobowe członków rodzin pracowników;
   c. dane osobowe kandydata do pracy;
   d. obsługa kadrowo-płacowa pracownika.
3. Grupa informacji dotycząca infrastruktury fizycznej i Teleinformatycznej:
   a. dane na temat postępowania w sytuacji krytycznej (ewakuacja)
   b. dane dotyczące stanu infrastruktury;
   c. dane o zabezpieczeniach systemu informatycznego;
   d. dane o zabezpieczeniach infrastruktury fizycznej;
   e. dane dotyczące systemów zarządzania;
   f. dokumentacja techniczna infrastruktury.
4. Grupa informacji dotycząca finansów przedszkola:
   a. informacje finansowe;
   b. dane z kontroli i audytów;
   c. informacje dotyczące kontrahentów.

Inspektor ochrony danych prowadzi *wykaz zbiorów danych* na podstawie, którego wydawane są upoważnienia do przetwarzania danych. Wykaz zbiorów danych w przedszkolu stanowi *załącznik nr 2* do Polityki bezpieczeństwa informacji i ochrony danych osobowych.
Na podstawie wykazu zbiorów tworzy się Rejestr czynności przetwarzania, który zgodnie z art. 30 RODO zawiera:

1. imię i nazwisko lub nazwę oraz dane kontaktowe administratora danych osobowych;
2. dane kontaktowe inspektora ochrony danych;
3. cele przetwarzania;
4. opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
5. kategorie odbiorów, którym dane osobowe zostały lub zostaną ujawnione;
6. jeżeli to możliwe planowane terminy usunięcia poszczególnych danych.

Rejestr czynności przetwarzania stanowi *załącznik nr 3 do Polityki Bezpieczeństwa i ochrony danych osobowych.*

§ 11

Środki organizacyjne i techniczne

Administrator danych osobowych jest zobowiązany zastosować środki techniczne i organizacyjne, zapewniające ochronę danych osobowych, adekwatne do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem – *wykaz zastosowanych środków organizacyjnych i technicznyc*h zastosowanych przez ADO stanowi *załącznik nr 10.*

Zastosowane środki organizacyjne i techniczne winny być adekwatne do oszacowanego ryzyka, którego kalkulacji dokonać należy poprzez *Ocenę skutków* – stanowiącą *załącznik nr 11 do Polityki*. Ocena ta zawiera: systematyczny opis planowanych operacji przetwarzania i ich celów, ocenę czy operację są niezbędne oraz proporcjonalne w stosunku do celów, ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, środki planowane w calu zaradzenia ryzyku, w tym mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia ogólnego UE.

§ 13

Instrukcje bezpieczeństwa przy przetwarzaniu danych osobowych dla osób upoważnionych oraz postępowania w sytuacji naruszenia danych określa *załącznik nr 12 do Polityki Bezpieczeństwa.*

§ 14

Mając na względzie ochronę danych osobowych uczniów oraz działając zgodnie z przepisami prawa wykorzystanie wizerunku oraz przetwarzanie danych osobowych dziecka w celach promocyjnych przedszkola może odbyć się wyłącznie za uprzednią zgodą rodzica stanowiącą *załącznik nr 13 do Polityki Bezpieczeństwa.*

§ 15

Ocena systemu ochrony danych

IOD jest zobowiązany do sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania w tym zakresie nie rzadziej niż raz w roku. Zakres sprawdzenia obejmuje przede wszystkim weryfikację wymagań zawartych:

- w Rozporządzeniu ogólnym o ochronie danych
- w przepisach krajowych dotyczących ochrony danych osobowych

poprzez:

- analizę kompletności oraz zgodności dokumentacji przetwarzania danych;
- stwierdzenia stanu faktycznego w zakresie przetwarzania danych;
- zgodności stanu faktycznego z przewidzianymi w dokumentacji środkami organizacyjnymi i technicznymi służącymi przeciwdziałaniu zagrożeniom dla ochrony danych osobowych.

§ 16

Obowiązek informacyjny

Administrator jest zobowiązany poinformować osobę, której dane dotyczą o przysługujących jej prawach oraz udzielić informacji- odnośnie przetwarzania jej danych osobowych zgodnie z art. 13 lub 14 RODO. W związku z tym administrator zawiera na wnioskach o przyjęcie do przedszkola i innych dokumentach, rozpoczynających daną sprawę klauzulę dotyczącą obowiązku informacyjnego, zawierającą w szczególności:

1. swoją tożsamość i dane kontaktowe;
2. dane kontaktowe inspektora ochrony danych;
3. cele przetwarzania danych oraz podstawę prawną;
4. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;
5. okres przez, który dane osobowe będą przechowywane;
6. informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania a także o prawie do przenoszenia danych;
7. informacje o prawie do cofnięcia zgody na przetwarzanie danych w dowolnym momencie;
8. informacje o prawie wniesienia skargi do organu nadzorczego.

Ponadto każdy z pracowników załatwiający indywidualną sprawę interesanta, rodzica ucznia, informuje go o jej prawach zgodnie z powyższym schematem. Czyni to zwłaszcza w tych przypadkach, gdy na wniosku, piśmie inicjującym sprawę nie zawarto klauzuli informacyjnej.

§ 17

Przetwarzanie danych w systemach informatycznych

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym określa odrębny dokument - *Polityka Bezpieczeństwa Systemów Teleinformatycznych*.

§ 18
Deklaracja Administratora

Realizując Politykę Bezpieczeństwa w zakresie ochrony danych osobowych Miejskie Przedszkole Nr 4 w Zambrowie dokłada szczególnej staranności w celu zapewnienia bezpieczeństwa przetwarzanych danych oraz zaangażowanie w podejmowanie przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.

1. Dyrektor Przedszkola, wykonując zadania Administratora Danych Osobowych, świadomy wagi problemów związanych z ochroną danych osobowych deklaruje:
   1.1. zapewnienie ochrony interesów osób, których dane dotyczą, a w szczególności, aby dane te były:
      a. przetwarzane zgodnie z prawem,
      b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu niezgodnemu z nimi przetwarzaniu,
      c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
      d. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
   1.2. inicjatywę podejmowania działań doskonalących i rozwijających techniczne i organizacyjne środki ochrony danych zapewniając skuteczne zapobieganie zagrożeniom,
   1.3. zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa danych osobowych,
   1.4. kontrolę i nadzór nad przetwarzaniem danych osobowych oraz nieustanne monitorowanie zmieniających się zagrożeń wewnętrznych i zewnętrznych, uwzględniając przy tym zmieniające się przepisy prawa.
2. Ze względu na nieustanną modyfikację zagrożeń oraz zmieniające się przepisy prawa Polityka Bezpieczeństwa może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych czynników stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

§ 19

Odpowiedzialność karna

1. Niezastosowanie się do prowadzonej przez administratora danych osobowych Polityki bezpieczeństwa informacji i ochrony danych osobowych, której założenia określa niniejszy dokument oraz naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące odpowiedzialnością dyscyplinarną lub rozwiązaniem stosunku pracy (na podst. art. 52 Kodeksu Pracy).
2. Niezależnie od stosunku pracy za przetwarzanie niezgodne z prawem, celem przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z krajowych przepisów dotyczących ochrony danych osobowych zawartych w art. 107 Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych

§ 20

Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

§ 21

Każda osoba, upoważniona do przetwarzania danych osobowych w Miejskim Przedszkolu Nr 4 w Zambrowie przed dopuszczeniem do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

§ 22

Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie. Udostępnienie niniejszego dokumentu może przyczynić się do utraty bezpieczeństwa danych, wskazując na podjęte zabezpieczenia oraz wdrożone środki organizacyjne i techniczne.

§ 23

Zapisy dokumentu Polityki Bezpieczeństwa wchodzą w życie z dniem 25.05.2018r.

……..

(pieczęć i podpis Administratora Danych Osobowych)