**Polityka Zarządzania Ryzykiem  
w procesie przetwarzania danych osobowych  
w Szkole Podstawowej im. Jana Pawła II   
w Jamielniku.**

**Rozdział 1**

**Postanowienia ogólne**

**§ 1**

**1**. Ilekroć w dokumencie jest mowa o:

* 1. **administratorze danych** – należy przez to rozumieć Dyrektora Szkoły Podstawowej im. Jana Pawła II w Jamielniku.
  2. **aktywach** – należy przez to rozumieć środki materialne i niematerialne mające wpływ   
     na przetwarzanie danych;
  3. **proces przetwarzania danych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych w celu określonego celu przetwarzania;
  4. **operacji przetwarzania danych** – należy przez to rozumieć każdą czynność wykonywaną   
     na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany   
     lub niezautomatyzowany, taka, jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawniane poprzez wysłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
  5. **ryzyku –** należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia;
  6. **zarządzanie ryzykiem** – należy przez to rozumieć realizowany przez administratora danych osobowych proces, którego celem jest identyfikacja potencjalnych ryzyk, które mogą mieć wpływ na realizację celów i zadań jednostki;
  7. **mapa ryzyka** – tabela (macierz) odzwierciedlająca ocenę siły oddziaływania   
     i prawdopodobieństwo wystąpienia zidentyfikowanego ryzyka w placówce;
  8. **ocena ryzyka** – należy przez to rozumieć czynność polegającą na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie projektowania systemu bezpieczeństwa danych;
  9. **kryteriach akceptacji ryzyka** – są to kryteria, które określają dopuszczalność ryzyka, zdefiniowane poprzez wartość progową. Akceptowaną wartością jest ryzyko tylko w zakresie   
     0 - 4, przy przyjętych 5 -stopniowych skalach szacowania prawdopodobieństwa wystąpienia ryzyka i jego skutków;
  10. **rejestr ryzyk** – należy przez to rozumieć dokument odzwierciedlający przeprowadzoną identyfikację i analizę ryzyk, a także przyjętą reakcję na ryzyko;
  11. **bezpieczeństwie informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
  12. **zdarzeniu związanym z bezpieczeństwem danych** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci,   
      który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem danych;
  13. **incydencie** związanym z bezpieczeństwem danych – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne zakłócenia zadań i zagrażają bezpieczeństwu danych;
  14. **zagrożeniu** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
  15. **podatność** – słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki;
  16. **dostępności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
  17. **integralności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
  18. **poufności** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
  19. **informatycznym nośniku danych** — należy przez to rozumieć materiał służący   
      do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
  20. **zasobach systemu teleinformatycznego** – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt   
      oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego   
 prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

**§ 2**

**1.** Polityka zarządzania ryzykiem w zakresie ochrony danych osobowych, zwana dalej „polityką zarządzania ryzykiem”, obejmuje:

1. zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
2. zasady i tryb identyfikacji ryzyka;
3. zasady i tryb dokonywania analizy ryzyka;
4. zasady określania właściwej reakcji na ryzyko.

**§ 3**

**1.** Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich samodzielnych stanowisk wskazanych w Regulaminie Organizacyjnym placówki.

**§ 4**

**1.** Zarządzanie ryzykiem jest procesem ciągłym i nie ogranicza się do działań określonych   
w § 2 ust. 1.

**§ 5**

**1**. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje  
 to poprzez:

1. rozpoznanie – czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się   
   z działalnością placówki w zakresie ochrony danych osobowych i dokonywanie ich pomiaru;
2. ocenę ryzyka i jego istotności, przy pomocy skali określonej w § 9;
3. zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;
4. kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów   
   i nałożonych zadań.

**Rozdział 2**

**Zakresy zadań i obowiązków**

**§ 6**

**1**. Za realizację polityki zarządzania ryzykiem odpowiada Dyrektor szkoły poprzez:

1. kształtowanie i wdrażanie polityki zarządzania ryzykiem;
2. nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem;
3. wyznaczanie poziomu akceptowalnego dla każdego ryzyka;
4. podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.

**2.** Pracownicy na samodzielnych stanowiskach odpowiadają za zarządzanie ryzykiem poprzez:

1. identyfikację ryzyk związanych z realizacją przydzielonych zadań w zakresie ochrony danych osobowych;
2. wskazywanie właścicieli zidentyfikowanych ryzyk;
3. przeprowadzanie analizy zidentyfikowanego ryzyka we współpracy z Inspektorem Ochrony Danych;
4. proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk;
5. wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyka.
   * 1. Pracownicy wymienieni w ust. 2 są zobowiązani do współpracy z dyrektorem szkoły.

**Rozdział 3**

**Identyfikacja ryzyka**

**§ 7**

**1**. Identyfikacja ryzyk prowadzona jest dla wszystkich zbiorów danych na poziomie jednostki i na poziomie poszczególnych samodzielnych stanowisk pracy.

**2.** W procesie identyfikacji ryzyka uwzględnia się zagrożenia. Ze względu na ich źródło ryzyka dzielą się na:

1. zewnętrzne – rodzaj ryzyka determinowanego przez czynniki zewnętrzne;
2. wewnętrzne – ryzyko to obejmuje działania wewnętrzne placówki i może być zarządzane wewnątrz jednostki.

**3.** Każde zidentyfikowane ryzyko ujmuje się w rejestrze, stanowiącym załącznik nr 2   
do Polityki Zarządzania Ryzykiem.

**4.** Dla każdego zidentyfikowanego ryzyka ustala się jego właściciela.

**5.** Każdy pracownik ma prawo i obowiązek zgłaszania swojemu bezpośredniemu przełożonemu ryzyk zidentyfikowanych podczas wykonywania przydzielonych zadań w zakresie ochrony danych osobowych.

**Rozdział 4**

**Analiza ryzyka**

**§ 8**

**1**. Każde ryzyko w zakresie ochrony danych osobowych podlega analizie pod kątem jego istotności na osiąganie celów i zadań. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

**2**. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia   
i skutku oddziaływania.

**3.** W celu dokonania oceny ryzyka wykorzystuje się Mapę Ryzyka, którą stanowi macierz prawdopodobieństwo – skutek – załącznik nr 3 do Polityki Zarządzania Ryzykiem.

**4.** Mapa ryzyka definiuje ryzyka na:

1. niskie o wartości 4 i mniejszej;
2. średnie o wartości powyżej 4 i mniejszej niż 9;
3. wysokie – o wartości powyżej 9 i mniejszej niż 16.
4. katastrofalne – o wartości powyżej 16.
5. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie;
6. 1 – oznacza skutek nieznaczny;
7. 2 – oznacza skutek mały;
8. 3 – oznacza skutek średni;
9. 4 – oznacza skutek poważny;
10. 5 – oznacza skutek katastrofalny.
11. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową   
    od 1 do 5, gdzie:
12. 1 – oznacza prawdopodobieństwo rzadkie (0-20 %);
13. 2 – oznacza prawdopodobieństwo małe (21 - 40%);
14. 3 – oznacza prawdopodobieństwo możliwe (41 - 60 %);
15. 4 – oznacza prawdopodobieństwo prawdopodobne (61 - 80 %);
16. 5 – oznacza prawdopodobieństwo prawie pewne (81 -100 %).
17. Wskaźniki do punktacji oceny prawdopodobieństwa i skutków ryzyka określa   
    załącznik nr 4.

**Rozdział 5**

**Reakcja na ryzyko**

**§ 9**

**1.** Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1. tolerowanie – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści, z zdolności   
   do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne;
2. przeniesienie – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług   
   na zewnątrz;
3. wycofanie się – dotyczyć to będzie grypy ryzyk dla których mimo podejmowanych działań   
   nie udało się zmniejszyć ich istotności do akceptowanego poziomu;
4. przeciwdziałanie – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji,   
   lub znacznego ograniczenia.

**Rozdział 6**

**Postanowienia końcowe.**

**§ 11**

**1**. Strategia zarządzania ryzykiem obowiązuje od 25 maja 2018 roku.

1. Pracownicy szkoły obowiązani są do systematycznej analizy wystąpienia ryzyk   
   na stanowiskach pracy i zgłaszania ich dyrektorowi szkoły.

***Załącznik do polityki Zarządzania Ryzykiem:***

1. *Załącznik nr 1 – Rejestr zbiorów*
2. *Załącznik nr 2 - Rejestr ryzyka w poszczególnych aktywach – wzór dokumentu;*
3. *Załącznik nr 3 - Mapa ryzyka – wzór dokumentu;*
4. *Załącznik nr 4 - Wskaźniki do szacowania prawdopodobieństwa i skutków.*