Załącznik nr 1 do zarządzenia nr 30/2016/2017 – „Procedura zarządzania ryzykiem w bezpieczeństwie informacji”

PROCEDURA ZARZĄDZANIA RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI

§ 1.

1. „Procedura zarządzania ryzykiem w bezpieczeństwie informacji”, zwana w dalszej części „Procedurą”, określa zasady przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, w Gimnazjum nr 12 im. Górniczego Stanu w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Gimnazjum nr 12 im. Górniczego Stanu w Rybniku lub osobę zastępującą,
   2) Gimnazjum – należy przez to rozumieć Gimnazjum nr 12 im. Górniczego Stanu w Rybniku,
   3) ryzyku – należy przez to rozumieć ryzyko w bezpieczeństwie informacji.

§ 2.

1. W Gimnazjum wyodrębnia się trzy grupy informacji:
   1) dane osobowe,
   2) arkusze egzaminacyjne Okręgowej Komisji Egzaminacyjnej,
   3) informacje niebędące danymi osobowymi lub arkuszami egzaminacyjnymi Okręgowej Komisji Egzaminacyjnej.
2. Poziom ochrony informacji szacuje się poprzez analizę poufności, integralności i dostępności dla rozważanej grupy informacji i przyjmuje się, że:
   1) dane osobowe i arkusze egzaminacyjne Okręgowej Komisji Egzaminacyjnej są informacjami poufnymi, chronionymi przed dostępem nieuprawnionych osób, dostępnymi w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją,
   2) informacje niebędące danymi osobowymi są informacjami ogólnodostępnymi lub dostępnymi na wniosek, w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją.
3. Zapewnienie poufności oznacza zabezpieczenie informacji przed dostępem nieuprawnionych osób, podmiotów lub procesów.
4. Zapewnienie dostępności oznacza możliwość wykorzystania informacji w dowolnym momencie przez uprawnioną osobę.
5. Zapewnienie integralności oznacza zabezpieczenie informacji przed nieuprawnioną modyfikacją.

§ 3.

1. Ryzyko to wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Ryzyko jest proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować.
2. Zarządzanie ryzykiem to skoordynowane działania dotyczące kierowania i nadzorowania Gimnazjum w odniesieniu do ryzyka. W ramach zarządzania ryzykiem analizuje się, co może się zdarzyć i jakie mogą być możliwe następstwa, a następnie podejmuje decyzję, co i kiedy należy wykonać, aby zredukować ryzyko do akceptowalnego poziomu.

§ 4.

1. Prawdopodobieństwo wystąpienia ryzyka jest to oczekiwana częstotliwość wystąpienia zdarzenia zdefiniowanego jako ryzyko.
2. Strata, którą może spowodować ryzyko jest to wpływ zdarzenia zidentyfikowanego jako ryzyko na integralność, dostępność lub poufność.

§ 5.

1. Ocena ryzyka polega na określeniu prawdopodobieństwa wystąpienia ryzyka i starty, którą może spowodować ryzyko.
2. Oceny ryzyka dokonuje się poprzez przyznanie prawdopodobieństwu wystąpienia ryzyka oraz stracie, którą może spowodować ryzyko, odpowiedniej liczby punktów, w oparciu o tabele punktowe i zsumowanie przyznanej liczby punktów. Dla straty, którą może spowodować ryzyko, przyjmuje się najwyższą przyznaną liczbę punktów spośród wszystkich kategorii.
3. Oceny ryzyka dokonuje się odrębnie dla każdej grupy informacji i dla utraty integralności, dostępności lub poufności informacji.
4. Tabela punktowa prawdopodobieństwa wystąpienia ryzyka utraty integralności, dostępności lub poufności informacji stanowi załącznik nr 1 do „Procedury”, a tabela punktowa straty, którą może spowodować ryzyko utraty integralności, dostępności lub poufności informacji – załącznik nr 2 do „Procedury”.
5. Oceny ryzyka występujące w Gimnazjum:
   a) ryzyko wysokie – suma przyznanych punktów od 8 do 10. Duża istotność. Konsekwencje poważne. Niezbędne są działania naprawcze,
   b) ryzyko średnie – suma przyznanych punktów od 5 do 7. Średnia istotność. Przeciwdziałanie wskazane,
   c) ryzyko niskie – suma przyznanych punktów od 1 do 4. Mała istotność. Przeciwdziałanie zależy od decyzji właściciela ryzyka.

§ 6.

1. W przypadku ryzyka wysokiego lub średniego konieczne jest postępowanie z ryzykiem.
2. Metody postępowania z ryzykiem występujące w Gimnazjum:
   a) unikanie – polega na dywersyfikacji, eliminacji, zakazie,
   b) zatrzymanie – polega na akceptacji i ponownej wycenie,

c) redukcja – polega na rozproszeniu,
d) transfer – polega na ubezpieczeniu, zabezpieczeniu, kompensacie,
e) wykorzystanie – polega na alokacji, ekspansji, przeprojektowaniu.

3. Postępowanie z ryzykiem powinno być proporcjonalne do ryzyka tak, aby, w większości przypadków, ryzyko mieć pod kontrolą, a nie je eliminować.
4. Postępując z ryzykiem należy brać pod uwagę w szczególności:
   1) ograniczenia czasowe (zabezpieczenie powinno zostać wdrożone w czasie życia informacji lub systemu),
   2) ograniczenia finansowe (zabezpieczenia nie powinny być bardziej kosztowne do wdrożenia lub utrzymania niż strata, którą może przynieść ryzyko, za wyjątkiem sytuacji, gdy osiągnięcie zgodności jest wymagane przepisami prawa),
   3) ograniczenia techniczne,
   4) ograniczenia kulturowe (jeśli pracownicy nie rozumieją zabezpieczenia lub nie akceptują go, to zabezpieczenie staje się z czasem nieskuteczne),
   5) ograniczenia prawne,
   6) łatwość użycia,
   7) ograniczenia przy integrowaniu nowych i istniejących zabezpieczeń.

§ 7.

1. Oceny ryzyka dokonuje zespół ds. oceny ryzyka w bezpieczeństwie informacji, który każdorazowo powołuje Dyrektor.
2. Ocenę ryzyka dokumentuje się z wykorzystaniem karty oceny ryzyka w bezpieczeństwie informacji, która stanowi załącznik nr 3 do „Procedury”.
3. Karty oceny ryzyka w bezpieczeństwie informacji stanowią rejestr ryzyka w bezpieczeństwie informacji.

§ 8.

W sprawach nieuregulowanych w „Procedurze” decyzję podejmuje Dyrektor.

Załącznik nr 1 do „Procedury zarządzania ryzykiem” – tabela punktowa prawdopodobieństwa wystąpienia ryzyka utraty integralności, dostępności lub poufności informacji

TABELA PUNKTOWA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA RYZYKA UTRATY INTEGRALNOŚCI, DOSTĘPNOŚCI LUB POUFNOŚCI INFORMACJI

Prawdopodobieństwo wystąpienia ryzyka	**Opis**	**Liczba punktów**
Bardzo niskie	Zdarzenie, którego zaistnienie jest wysoce nieprawdopodobne (0% – 20%)	1
Niskie	Zdarzenie, którego zaistnienie jest mało prawdopodobne (21% – 40%)	2
Średnie	Zdarzenie, którego zaistnienie jest względnie prawdopodobne (41% – 60%)	3
Wysokie	Zdarzenie, którego zaistnienie jest dość prawdopodobne (61% – 80%)	4
Bardzo wysokie	Zdarzenie, którego zaistnienie jest bardzo prawdopodobne (81% – 100%)	5

Załącznik nr 2 do „Procedury zarządzania ryzykiem” – tabela punktowa straty, którą może spowodować ryzyko utraty integralności, dostępności lub poufności informacji

TABELA PUNKTOWA STRATY, KTÓRĄ MOŻE SPOWODOWAĆ RYZYKO UTRATY INTEGRLNOŚCI, DOSTĘPNOŚĆI LUB POUFNOŚCI INFORMACJI

Stopień oddziaływania ryzyka	**Kryteria**			**Liczba punktów**
	Skutki finansowe	**Odpowiedzialność za zaistnienie zdarzenia**	**Reputacja**	
Bardzo niski	Od 100 zł do 1.000 zł	Brak naruszenia przepisów prawa	Brak informacji w mediach	1
Niski	Od 1.000 zł do 10.000 zł	Naruszenie przepisów prawa – brak odpowiedzialności	Informacja w mediach lokalnych	2
Średni	Od 10.000 zł do 100.000 zł	Złamanie przepisów prawa – odpowiedzialność służbowa	Informacja w mediach regionalnych	3
Wysoki	Od 100.000 zł do 250.000 zł	Złamanie przepisów prawa – odpowiedzialność służbowa i finansowa	Informacja w mediach ogólnokrajowych	4
Bardzo wysoki	Od 250.000 zł	Złamanie przepisów prawa – odpowiedzialność karna, ograniczenie lub pozbawienie wolności	Doniesienia medialne w całym kraju	5