

PROCEDURA ZARZĄDZANIA RYZYKIEM W GMINNYM OŚRODKU KULTURY W SMOŁDZINIE

§ 1.

Postanowienia ogólne

Ustala się zasady zarządzania ryzykiem w Gminnym Ośrodku Kultury w Smołdzinie.

1. Procedura swym zakresem obejmuje:
 - 1) identyfikację ryzyka dla wyznaczonych celów;
 - 2) identyfikację ryzyka dla działalności Ośrodka.
2. Celem zastosowania procedury zarządzania ryzykiem jest:
 - 1) usprawnienie procesu zarządzania Ośrodkiem;
 - 2) zwiększenie prawdopodobieństwa realizacji zadań i osiągnięcia założonych celów;
 - 3) zapewnienie odpowiednich mechanizmów kontroli zarządczej;
 - 4) zapewnienie Dyrektorowi Gminnego Ośrodka Kultury w Smołdzinie otrzymania na czas wczesnej informacji na temat zagrożenia dla funkcjonowania jednostki oraz realizacji założonych celów i zadań.

Niniejsza procedura określa zasady i formy identyfikacji ryzyka i analizy ryzyka, a także przebieg tego procesu w Gminnym Ośrodku Kultury w Smołdzinie.

3. System zarządzania ryzykiem podlega w sposób ciągły elastycznemu dostosowaniu do zmieniających się potrzeb i uwarunkowań prawnych.

§ 2.

Ilekroć w niniejszej Procedurze jest mowa o:

- 1) **Dyrektorze, kierowniku jednostki** – należy przez to rozumieć Dyrektora Gminnego Ośrodka Kultury w Smołdzinie;
- 2) **Jednostce, Ośrodku** – należy przez to rozumieć Gminny Ośrodek Kultury w Smołdzinie;
- 3) **Pracownikach** – należy przez to rozumieć pracowników zatrudnionych w Gminnym Ośrodku Kultury w Smołdzinie;
- 4) **Ryzyku** – należy przez to rozumieć kombinacje prawdopodobieństwa wystąpienia zdarzenia oraz jego skutków. We wszelkiego rodzaju przedsięwzięciach istnieje możliwość wystąpienia zdarzeń pociągających za sobą skutki, które stanowią szanse na dodatkowe korzyści bądź też zagrożenie dla prowadzenia przedsięwzięcia.

§ 3.

1. Ustala się następujące etapy zarządzania ryzykiem w Gminnym Ośrodku Kultury w Smołdzinie:
 - 1) identyfikacja ryzyka;
 - 2) analiza zidentyfikowanego ryzyka;
 - 3) punktowa ocena ryzyka;

- 4) określenie reakcji na ryzyko;
- 5) monitorowanie poziomu występującego ryzyka.
2. Dyrektor może wyznaczyć osobę/zespół, który będzie odpowiedzialny za koordynację systemu zarządzania ryzykiem.
3. Wyznaczenie osoby/zespołu nie zmienia ostatecznej odpowiedzialności Dyrektora za zarządzanie Ośrodkiem.

§ 4. Identyfikacja ryzyka

1. W Ośrodku proces identyfikacji ryzyka odbywa się ostatniego dnia listopada danego roku. W przypadku zaistnienia zmian organizacyjnych jednostki, zmian przepisów prawa obejmujących działalność jednostki, warunków funkcjonowania jednostki, wystąpienie nowego rodzaju ryzyka dokonuje się ponownej identyfikacji ryzyka.
2. Identyfikacja ryzyka w Ośrodku odbywa przy wyznaczaniu celów i zadań przyjętych w planie działalności na dany rok w kontekście szans oraz zagrożeń dla ich realizacji, występujących zarówno czynników wewnętrznych i zewnętrznych, zgodnie z przyjętymi w jednostce: *Zasadami i trybem wyznaczania celów jednostki, określenie mierników ich realizacji oraz zasad monitorowania ich osiągnięć w Gminnym Ośrodku Kultury w Smołdzinie* wprowadzonych Zarządzeniem Dyrektora Gminnego Ośrodka Kultury w Smołdzinie.
3. Przy identyfikacji ryzyka brane są pod uwagę następujące czynniki zewnętrzne i wewnętrzne:

CZYNNIKI ZEWNĘTRZNE	CZYNNIKI WEWNĘTRZNE
1. Zmieniające się oczekiwania lub potrzeby mieszkańców gminy. 2. Zmiany przepisów prawa mających wpływ na funkcjonowanie jednostki. 3. Zmiany gospodarcze. 4. Zmiany technologii. 5. Zagrożenia naturalne. 6. Naciski na jednostkę z zewnątrz.	1. Charakter prowadzonej jednostki. 2. Dostępne środki finansowe. 3. Komunikacja w jednostce. 4. Liczba pracowników i ich kwalifikacje. 5. Liczba, rodzaj i wielkość dokonywanych operacji finansowych. 6. Systemy informatyczne. 7. Kultura organizacji. 8. Plany i strategię. 9. Odpowiedzialność i postawa kierownictwa. 10. Przetwarzanie informacji.

4. Przy identyfikacji ryzyka brane są pod uwagę informacje wynikające z:
 - 1) sprawozdań z audytów i kontroli;
 - 2) skarg wpływających do Ośrodka;
 - 3) budżet i finanse;
 - 4) rejestr zdarzeń (dzienniki wypadków);
 - 5) projekty/programy;
 - 6) ankiety.

5. W procesie identyfikacji ryzyka uczestniczą wybrani pracownicy Ośrodka wypełniając ankietę zgodnie z **załącznikiem nr 1** do niniejszej procedury.
6. Dla zidentyfikowanego ryzyka Dyrektor bądź zespół do tego wyznaczony prowadzi rejestr ryzyka zgodnie z **załącznikiem nr 2** do niniejszej procedury, na podstawie ankiet wypełnionych przez pracowników Ośrodka.
7. Każdy pracownik ma prawo i obowiązek zgłaszania swojemu bezpośredniemu przełożonemu bądź zespołowi ds. zarządzania ryzykiem ryzyka zidentyfikowanych podczas wykonywania swoich obowiązków i przydzielonych zadań.
8. Ryzyka identyfikowane są w ramach najistotniejszych obszarów działania Ośrodka. Wykaz obszarów działania jednostki określa **załącznik nr 4** do niniejszej procedury.
9. Do zidentyfikowanego ryzyka określa się kategorie ryzyk. Jako kategorie ryzyka stosuje się:
 - 1) ryzyko działalności;
 - 2) ryzyko zasobów ludzkich;
 - 3) ryzyko finansowe;
 - 4) ryzyko zewnętrzne.
10. Wykaz kategorii ryzyk określa **załącznik nr 5** do niniejszej procedury.

§ 5.

Analiza zidentyfikowanego ryzyka

1. Analiza zidentyfikowanego ryzyka oznacza:
 - 1) ocenę siły oddziaływania (skutku) ryzyka poprzez przypisanie każdemu z ryzyka wartości punktowej;
 - 2) ocenę prawdopodobieństwa wystąpienia ryzyka poprzez przypisanie każdemu z ryzyka wartości punktowej.
2. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

$$R = P \times S$$

gdzie:

R – poziom ryzyka

P – Prawdopodobieństwo wystąpienia zdarzenia

S – Skala oddziaływania w przypadku wystąpienia zdarzenia (Skutek)

3. Oceniając prawdopodobieństwo wystąpienie ryzyka uwzględnia się możliwą częstotliwość wystąpienia zdarzenia. W odniesieniu do czynności powtarzalnych (spraw występujących cyklicznie lub wielokrotnie) uwzględnia się liczbę możliwych powtórzeń (ile razy względem ogólnej liczby spraw zdarzenie może mieć miejsce).
4. Sposób oceny prawdopodobieństwa wystąpienia ryzyka:

Prawdopodobieństwo	Odpowiednik punktowy	Przesłanki
Bardzo duże	5	Oczekuje się, że zdarzenie takie nastąpi (od 81 do 100%, że będzie występować regularnie, co miesiąc lub częściej), dotyczy wszystkich lub prawie wszystkich spraw.
Duże	4	Zaistnienie zdarzenia jest bardzo prawdopodobne (od 61 do 80 %, że wystąpi regularnie, co najmniej raz w roku), dotyczy większości spraw.
Średnie	3	Zaistnienie zdarzenia jest średnio możliwe, ale w niektórych przypadkach zdarzenie takie może mieć miejsce (od 41 do 60%, że wystąpi w przeciągu 5 lat), dotyczy niektórych spraw.
Małe	2	Istnieje małe prawdopodobieństwo zaistnienia tego zdarzenia (od 21 do 40%, że wystąpi raz na 5 lat), może wystąpić kilka razy w okresie 5 lat, dotyczy nielicznych spraw.
Bardzo małe	1	Zdarzenie może zaistnieć jedynie w wyjątkowych okolicznościach (od 1 do 20%, że wystąpi raz na 10 lat), a najprawdopodobniej w ogóle nie wystąpi, nie wystąpiło dotychczas, dotyczy jednostkowych spraw.

5. Ocena skutków wystąpienia ryzyka opiera się na oszacowaniu potencjalnych skutków, a więc wyników oddziaływania, jakie zaistnienie danego rodzaju ryzyka może mieć na jednostkę i realizację jej celów i zadań. Uwzględnia się przy tym w szczególności konsekwencje prawne, finansowe i organizacyjne zaistnienia danego zdarzenia oraz jego wpływ na wizerunek jednostki i bezpieczeństwo pracowników.
6. Sposób oceny skutku ryzyka:

Skutek wystąpienia ryzyka	Odpowiednik punktowy	Przesłanki
Katastrofalny	5	Brak realizacji zadania i brak realizacji celu, bardzo poważne i rozległe konsekwencje prawne, naruszenie bezpieczeństwa pracowników (ujemne konsekwencje dla zdrowia i życia pracowników), wysokie straty finansowe, utrata dobrego wizerunku jednostki. (Wysoka strata finansowa – powyżej 1% budżetu jednostki)
Poważny	4	Poważny wpływ na realizację zadania w tym poważne zagrożenie terminu jego realizacji, jaki i osiągnięcie celu, poważne konsekwencje prawne, zagrożenie bezpieczeństwa pracowników, poważne straty finansowe, poważny wpływ na wizerunek jednostki. (Poważny skutek finansowy – od 0,5% do 1% budżetu jednostki)

Średni	3	Średni wpływ na realizację zadań i celów, umiarkowane konsekwencje prawne, średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek jednostki. (Średni skutek finansowy – od 0,2% do 0,5% budżetu jednostki)
Mały	2	Mały wpływ na realizację celów i zadań, bez skutków prawnych, mały skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek jednostki. (Mały skutek finansowy – od 0,1% do 0,2% budżetu jednostki)
Nieznacznym	1	Znikomy wpływ na realizację zadań i celów, brak skutków prawnych, nieznacznym skutek finansowy, brak wpływu na bezpieczeństwo pracowników, brak wpływu na wizerunek jednostki. (Nieznacznym skutek finansowy do 0,1 % budżetu jednostki)

7. W celu dokonania oceny ryzyka wykorzystuje się mapę istotności ryzyka, która stanowi macierz prawdopodobieństwo-skutek.

Prawdopodobieństwo					
Bardzo duże	5	10	15	20	25
Duże	4	8	12	16	20
Średnie	3	6	9	12	15
Małe	2	4	6	8	10
Bardzo małe	1	2	3	4	5
	Nieznacznym	Mały	Średni	Poważnym	Katastrofalnym
					Skutek

8. Poziomy istotności ryzyka:

Istotność	P x S	Charakter ryzyka	Reakcja na ryzyko
Istotne	16-25	Wysoki wpływ ryzyka, ryzyko prawie pewne lub możliwe; Średni wpływ ryzyka, ryzyko prawie pewne.	W przypadku niemożności odstąpienia od realizacji bezzwłocznie zaplanować i zrealizować odpowiedź na ryzyko.
Średnio istotne	5-15	Wysoki wpływ ryzyka, ryzyko incydentalne; Średni wpływ ryzyka, ryzyko możliwe lub incydentalne; Niski wpływ ryzyka, ryzyko prawie pewne.	Zaplanować odpowiedź na ryzyko, zaplanowane działania zapobiegawcze zrealizować w momencie przystąpienia do realizacji określonych działań operacyjnych.

Niskie	1-4	Niski wpływ ryzyka, ryzyko możliwe lub incydentalne.	Monitorować ryzyko, zaplanować i zrealizować odpowiedź na ryzyko w przypadku zaistnienia symptomów wystąpienia określonego ryzyka.
---------------	------------	--	--

9. Ryzykiem akceptowalnym jest ryzyko niskie.
10. Ryzyko przekraczające akceptowalny poziom wymaga ustalenia i podjęcia działań ograniczających je do poziomu akceptowalnego.
11. Dla ryzyka istotnego o wartości od 16 do 25 punktów konieczne jest wycofanie się z działania do czasu obniżenia poziomu ryzyka.
12. Dla ryzyka stosuje się odpowiednie mechanizmy kontroli w celu obniżenia istniejącego ryzyka.

§ 6.

1. Mechanizmy kontrolne to działania zaradcze, które mają na celu ograniczenie ryzyka do akceptowalnego – zarówno prawdopodobieństwo jak i skutek jego wystąpienia.
2. Do mechanizmów kontroli należy:
 - 1) dokumentowanie systemu kontroli zarządczej (procedury, instrukcje, zarządzenia, zakresy czynności, regulamin organizacyjny);
 - 2) dokumentowanie i rejestrowanie operacji finansowych i gospodarczych;
 - 3) nadzór;
 - 4) ciągłość działalności;
 - 5) ochrona zasobów;
 - 6) mechanizmy kontroli dotyczące systemów informatycznych.
3. Wyniki analizy ryzyka oraz wybór reakcji na ryzyko są udokumentowane w rejestrze ryzyka.

§ 7.

1. Dla każdego istotnego zidentyfikowanego i poddanego analizie ryzyka Dyrektor wskazuje optymalną, jego zdaniem, reakcję:
 - 1) **Tolerowanie** – w przypadku, gdy możliwość przeciwdziałania jest ograniczona lub koszty podjętych działań mogą przekroczyć przewidywane korzyści, a także gdy poziom ryzyka jest akceptowalny;
 - 2) **Przeniesienie** – dotyczyć to będzie kategorii ryzyka w odniesieniu do których nastąpi przeniesienie ich na inną instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz;
 - 3) **Działanie** – dotyczyć to będzie kategorii ryzyka, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do zminimalizowania ryzyka do akceptowalnego poziomu lub jego likwidacji
 - 4) **Wycofanie się** – dla zadań, w których nie można zmniejszyć wysokości ryzyka

- i których niepowodzenie naraża jednostkę na duże straty.
2. Wybór reakcji na ryzyko dokumentuje się w rejestrze ryzyka.
 3. Rejestr ryzyka jest sporządzony **do końca grudnia** danego roku przez Dyrektora Gminnego Ośrodka Kultury.

§ 8.

1. Zarządzanie ryzykiem jest procesem ciągłym. Zidentyfikowane ryzyko oraz ustalone metody jego ograniczenia są na bieżąco analizowane przez kierownictwo jednostki w ramach bieżącego zarządzania Ośrodkiem.
2. Wyniki oceny i analizy ryzyka wykorzystywane są na bieżąco do poprawy efektywności zarządzania ryzykiem oraz usprawnienia systemu zarządzania jednostką.

§ 9.

1. Przed sporządzeniem rejestru ryzyka na rok następny **do 15 grudnia** danego roku sporządza się sprawozdanie z zarządzania ryzykiem, w którym określa się, czy dane ryzyko wystąpiło, jakie działania zostały podjęte oraz jakie działania są planowane (jeśli są planowane).
2. Sprawozdanie, w którym mowa w ust. 1 dołącza się do rejestru ryzyka na rok, którego dotyczy. Wzór sprawozdania stanowi **załącznik nr 3** do niniejszej procedury.

ZAŁĄCZNIK NR 1 do Procedury
zarządzania ryzykiem w Gminnym
Ośrodku Kultury w Smółdzinie

Wzór ankiety służącej do identyfikacji ryzyka

Lp.	Ryzyko	Wystąpienie ryzyka		Uwagi
		Tak	Nie	
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

REJESTR RYZYKA

Lp.	Obszar działania Jednostki	Ryzyko	Kategoria ryzyka wg. Załącznika nr 5	Właściciel ryzyka	Ocena ryzyka przed podjęciem działań profilaktycznych			Działania profilaktyczne mające na celu wyeliminowanie lub zmniejszenie ryzyka (mechanizmy kontroli)	Ocena ryzyka po podjęciu działań profilaktycznych		
					P	S	Istotność		P	S	Istotność
					6	7	8		10	11	12
1											
2											
3											
4											

.....
(Miejscowość, data)

.....
(Podpis Dyrektora)

ZAŁĄCZNIK NR 3 do Procedury zarządzania
ryzykiem w Gminnym Ośrodku Kultury w
Smółdzinie

SPRAWOZDANIE Z ZARZĄDZANIA RYZYKIEM

[illegible]

**Wykaz najistotniejszych obszarów funkcjonowania
Gminnego Ośrodka Kultury w Smołdzinie**

Lp.		Obszar działania Ośrodka
1.	DZIAŁALNOŚĆ PODSTAWOWA (Statutowa)	Działalność kulturalna
2.	DZIAŁALNOŚĆ POMOCNICZA	Bezpieczeństwo
		Finanse i budżet
		Gospodarowanie mieniem
		Struktura organizacyjna
		Zasoby ludzkie
		Przepływ informacji
		Systemy informatyczne
		Zamówienia publiczne

Kategorie ryzyka

Poniższa tabela przedstawia kategorie ryzyka wraz z przykładami dotyczącymi jego możliwych źródeł (przyczyn) oraz skutków. Tabela nie określa zamkniętego katalogu ryzyka.

Oznaczenie	Ryzyko finansowe	
RF.1	Budżetowe	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów.
RF.2	Oszustwa i kradzieże	Związane ze stratą środków rzeczowych i finansowych będącą wynikiem przestępstwa lub wykroczenia.
RF.3	Podlegające ubezpieczeniu	Związane ze stratami finansowymi, które mogą być przedmiotem ubezpieczenia, np. ryzyko pożaru, wypadku.
RF.4	Zamówień publicznych i zlecania zadań publicznych	Związane z podejmowaniem decyzji oraz udzielaniem zamówień publicznych lub zlecaniem zadań publicznych innym podmiotom, np. ryzyko naruszenia zasad, form lub trybu ustawy o zamówieniach publicznych.
RF.5	Odpowiedzialności	Związane z obowiązkiem zapłaty kwot pieniężnych tytułem np. odszkodowań, odsetek karnych, kosztów procesowych.
RF.6	Realizacja programów współfinansowanych ze środków UE	Związane z wystąpieniem nieprawidłowości przy wykorzystaniu środków z UE.
Ryzyko dot. zasobów ludzkich		
RZL.1	Zarządzanie zasobami ludzkimi	Związane z liczebnością i kompetencjami pracowników, szkoleniami, wprowadzaniem nowych zadań bez zabezpieczenia etatowego.
RZL.2	BHP	Związane ze zdrowiem pracowników i wypadkami przy pracy.
Ryzyko działalności		
RD.1	Regulacji wewnętrznych i zewnętrznych	Związane z istnieniem i adekwatnością regulacji wewnętrznych i zewnętrznych.
RD.2	Organizacji i podejmowania decyzji	Związane ze strukturą organizacyjną, organizacją pracy oraz przekazywaniem obowiązków i uprawnień, np. ryzyko nieprecyzyjnie określonych obowiązków, ryzyko braku formalnie powierzonych obowiązków, ryzyko nieodpowiedniej struktury organizacyjnej, ryzyko nieprawidłowo wydanej decyzji.
RD.3	Kontroli wewnętrznej	Związane z funkcjonowaniem systemu kontroli wewnętrznej, np. ryzyko niedostatecznej kontroli, ryzyko nieskutecznych mechanizmów kontrolnych /działań zaradczych.
RD.4	Informacji	Związane z jakością informacji, na podstawie których podejmowane są decyzje, np. ryzyko braku komunikacji wewnętrznej i zewnętrznej.
RD.5	Reputacji	Związane z reputacją Ośrodka, np. ryzyko negatywnych opinii.
Ryzyko bezpieczeństwa informacji		

RB.1	Ochrony informacji (w tym danych osobowych) przetwarzanych w jednostce	Związane z zapewnieniem bezpieczeństwa informacji przetwarzanych w jednostce zarówno w formie papierowej, jak i elektronicznej, np. nadanie użytkownikom nadmiarowych bądź niewystarczających uprawnień, ujawnienie poufnych danych ze względu na nieadekwatny poziom zabezpieczeń logicznych lub fizycznych, nieadekwatne działania w związku z wystąpieniem incydentów bezpieczeństwa informacji, nieskuteczne zabezpieczenia fizyczne i środowiskowe, utrata istotnych danych wymaganych w realizacji zadań Ośrodka ze względu na awarię sprzętu i/lub oprogramowania, nieautoryzowana modyfikacja poufnych danych w wyniku wykorzystania podatności systemów przez atakującego, naruszenie zasad bezpieczeństwa przez zewnętrznego dostawcę, brak wiedzy na temat aktualnego stanu bezpieczeństwa
RB.2	Ciągłości działania	Związane np. z brakiem odpowiednich kompetencji do zapewnienia ciągłości działania zadań Ośrodka.
Ryzyko zewnętrzne		
RZ.1	Infrastruktury	Związane z infrastrukturą, np. wyposażeniem, bazą lokalową, środkami transportu i środkami łączności.
RZ.2	Środowiska prawnego	Związane ze skomplikowaniem i zmianami prawa oraz niejednolitym orzecnictwem.