

**ZARZĄDZENIE NR 14/2021**  
**WÓJTA GMINY JEŻEWO**

z dnia 1 lutego 2021 r.

**w sprawie wprowadzenia Procedury zarządzania ryzykiem w Urzędzie Gminy Jeżewo**

Na podstawie art. 68 ust. 1, ust. 2 pkt 7 ustawy z dnia 27 sierpnia 2009 roku o finansach publicznych (Dz. U. z 2019 r. poz. 869 z późn. zm.) oraz w oparciu o Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 roku w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Ministra Finansów z dnia 30 grudnia 2009 r., Nr 15, poz. 84) i w oparciu o Komunikat Nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (Dz. Urz. Ministra Finansów z dnia 18 grudnia 2012 r., poz. 56) zarządza się, co następuje:

§ 1. Przyjmuje się do stosowania *Procedurę zarządzania ryzykiem w Urzędzie Gminy Jeżewo* w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2. Do zapoznania się z niniejszym zarządzeniem i przyjęciem do stosowania zobowiązani są wszyscy pracownicy Urzędu.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Jeżewo

**Maciej Rakowicz**

Załącznik do zarządzenia Nr 14/2021

Wójta Gminy Jeżewo

z dnia 1 lutego 2021 r.

## **PROCEDURA ZARZĄDZANIA RYZYKIEM W URZĘDZIE GMINY JEŻEWO**

Data i miejsce sporządzenia dokumentu:	
Zatwierdził:	

## § 1. Postanowienia ogólne

1. Ustala się zasady zarządzania ryzykiem w Urzędzie Gminy Jeżewo.
2. Procedura swym zakresem obejmuje:
  - 1) identyfikację ryzyka dla wyznaczonych celów;
  - 2) identyfikację ryzyka dla działalności jednostki.
3. Celem zastosowania procedury zarządzania ryzykiem jest:
  - 1) usprawnienie procesu zarządzania Urzędem;
  - 2) zwiększenie prawdopodobieństwa realizacji zadań i osiągnięcia założonych celów;
  - 3) zapewnienie odpowiednich mechanizmów kontroli zarządczej;
  - 4) zapewnienie Wójtowi otrzymania na czas wczesnej informacji na temat zagrożenia dla funkcjonowania jednostki oraz realizacji założonych celów i zadań.
4. Niniejsza procedura określa zasady i formy identyfikacji ryzyka i analizy ryzyka, a także przebieg tego procesu w Urzędzie.
5. System zarządzania ryzykiem podlega w sposób ciągły elastycznemu dostosowaniu do zmieniających się potrzeb i uwarunkowań prawnych.

## § 2.

Ilekróć w niniejszej Procedurze jest mowa o:

- 1) **Wójt** – należy przez to rozumieć Wójta Gminy Jeżewo;
- 2) **Jednostce, Urzędzie** – należy przez to rozumieć Urząd Gminy Jeżewo;
- 3) **Kierownikach komórek organizacyjnych** – należy przez to rozumieć Kierowników Referatów Urzędu lub samodzielne stanowiska;
- 4) **Ryzyku** – należy przez to rozumieć prawdopodobieństwo wystąpienia zdarzenia, które będzie miało negatywny wpływ na realizację zadań statutowych jednostki bądź osiągnięcie założonych celów.

## § 3.

1. Ustala się następujące etapy zarządzania ryzykiem w Urzędzie Gminy Jeżewo:
  - 1) identyfikacja ryzyka;
  - 2) analiza zidentyfikowanego ryzyka;
  - 3) punktowa ocena ryzyka;
  - 4) określenie reakcji na ryzyko;
  - 5) monitorowanie poziomu występującego ryzyka.
2. Sekretarz jest odpowiedzialny za koordynację systemu zarządzania ryzykiem.
3. Wyznaczenie Sekretarza jako koordynatora nie zmienia ostatecznej odpowiedzialności Wójta za zarządzanie jednostką.

## § 4.

### Identyfikacja ryzyka

1. W Urzędzie Gminy proces identyfikacji ryzyka odbywa się w styczniu danego roku. W przypadku zaistnienia zmian organizacyjnych jednostki, zmian przepisów prawa obejmujących działalność jednostki, warunków funkcjonowania jednostki, wystąpienia nowego rodzaju ryzyka dokonuje się ponownej identyfikacji ryzyka.
2. Identyfikacja ryzyka w Urzędzie 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 Urzędzie Gminy Jeżewo” wprowadzonych Zarządzeniem nr 15/2021 Wójta Gminy Jeżewo z dnia 1 lutego 2021 r.
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. 3. Zmiany gospodarcze. 4. Zmiany technologii. 5. Zagrożenia naturalne.	1. Charakter działalności 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.

4. Przy identyfikacji ryzyka brane są pod uwagę informacje wynikające:
  - 1) ze sprawozdań z audytów i kontroli;
  - 2) ze skarg wpływających do jednostki;
  - 3) z budżetu i finansów;
  - 4) z rejestru zdarzeń (dzienniki wypadków);
  - 5) z projektów/programów;
  - 6) z ankiet.
5. W procesie identyfikacji ryzyka mogą uczestniczyć Kierownicy komórek organizacyjnych zgłaszając zidentyfikowane ryzyka Sekretarzowi.
6. Dla zidentyfikowanego ryzyka Sekretarz prowadzi rejestr ryzyka zgodnie z załącznikiem nr 1 do niniejszej procedury, na podstawie ankiet wypełnionych przez pracowników jednostki. Rejestr ryzyk Sekretarz przedstawia Wójtowi do zaakceptowania.
7. Przykładowe kategorie ryzyka, które mogą wystąpić w jednostce, przedstawia tabela stanowiąca załącznik nr 3. Tabela nie określa zamkniętego katalogu ryzyka, które mogą wystąpić w jednostce.

## § 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
<b>Bardzo duże</b>	<b>5</b>	Oczekuje się że zdarzenie takie nastąpi (od 81 do 100%, że będzie występować regularnie, co miesiąc lub częściej), dotyczy wszystkich lub prawie wszystkich spraw.
<b>Duże</b>	<b>4</b>	Zaistnienie zdarzenia jest bardzo prawdopodobne (od 61 do 80 %, że wystąpi regularnie, co najmniej raz w roku), dotyczy większości spraw.
<b>Średnie</b>	<b>3</b>	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.
<b>Małe</b>	<b>2</b>	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.
<b>Bardzo małe</b>	<b>1</b>	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 bezpieczeństwa pracowników.
6. Sposób oceny skutku ryzyka:

Skutek wystąpienia ryzyka	Odpowiednik punktowy	Przesłanki
<b>Katastrofalny</b>	<b>5</b>	<p>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.</p> <p>(Wysoka strata finansowa – powyżej 1% budżetu jednostki)</p>
<b>Poważny</b>	<b>4</b>	<p>Poważny wpływ na realizację zadania w tym poważne zagrożenie terminu jego realizacji, jak i osiągnięcia celu, poważne konsekwencje prawne, zagrożenie bezpieczeństwa pracowników, poważne straty finansowe, poważny wpływ na wizerunek jednostki.</p> <p>(Poważny skutek finansowy – od 0,5% do 1% budżetu jednostki)</p>
<b>Średni</b>	<b>3</b>	<p>Średni wpływ na realizację zadań i celów, umiarkowane konsekwencje prawne, średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek jednostki.</p> <p>(Średni skutek finansowy – od 0,2% do 0,5% budżetu jednostki)</p>
<b>Mały</b>	<b>2</b>	<p>Mały wpływ na realizację celów i zadań, bez skutków prawnych, mały skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek jednostki.</p> <p>(Mały skutek finansowy – od 0,1% do 0,2% budżetu jednostki)</p>
<b>Nieznacznym</b>	<b>1</b>	<p>Znikomy wpływ na realizację zadań i celów, brak skutków prawnych, nieznaczny skutek finansowy, brak wpływu na bezpieczeństwo pracowników, brak wpływu na wizerunek jednostki.</p> <p>(Nieznacznym skutek finansowy do 0,1 % budżetu jednostki)</p>

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	Poważny	Katastrofalny	<b>Skutek</b>

8. Poziomy istotności ryzyka:

Istotność	P x S	Charakter ryzyka	Reakcja na ryzyko
<b>Istotne</b>	<b>16-25</b>	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.
<b>Średnio istotne</b>	<b>5-15</b>	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.
<b>Niskie</b>	<b>1-4</b>	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 średnio istotnego 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 wskazuje się optymalną 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** – dotyczy 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** – dotyczy 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 sporządzany do końca stycznia danego roku przez Sekretarza, a następnie zostaje on zatwierdzony przez Wójta Gminy Jeżewo.

## § 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 jednostką.
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 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, o którym mowa w ust. 1 dołącza się do rejestru ryzyka na rok, którego dotyczy. Wzór sprawozdania stanowi **załącznik nr 2** do niniejszej procedury.

## REJESTR RYZYKA

Lp.	Ryzyko wraz z podaniem kategorii	Ocena ryzyka przed podjęciem działań profilaktycznych			Reakcja na ryzyko	Działania profilaktyczne mające na celu wyeliminowanie lub zmniejszenie ryzyka	Mechanizmy kontrolne
		Prawdopodobieństwo	Skutek	Istotność			
1	2	3	4	5	6	7	9
1							
2							
3							
4							

Jeżewo, dn. ....

.....  
Podpis Wójta

## SPRAWOZDANIE Z ZARZĄDZANIA RYZYKIEM

Lp.	Ryzyko wraz z podaniem kategorii	Istotność ryzyka przed podjęciem działań profilaktycznych	Reakcja na ryzyko	Ocena ryzyka po podjęciu działań profilaktycznych			Czy ryzyko się zmaterializowało?	Uwagi na rok następny
				Prawdopodobieństw 0	Skutek	Istotność		
1	2	3	4	5	6	7	8	9
1								
2								
3								
4								

Jeżewo, dn. ....

.....

Podpis Wójta

## Kategorie ryzyka

Poniższa tabela przedstawia kategorie ryzyka wraz z przykładami dotyczącymi jego możliwych źródeł (przyczyn) oraz skutków.

Tabela nie określa zamkniętego katalogu ryzyka.

<b>Ryzyko finansowe</b>	
<b>Budżetowe</b>	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów.
<b>Oszustwa i kradzieży</b>	Związane ze stratą środków rzeczowych i finansowych będącą wynikiem przestępstwa lub wykroczenia.
<b>Podlegające ubezpieczeniu</b>	Związane ze stratami finansowymi, które mogą być przedmiotem ubezpieczenia, np. ryzyko pożaru, wypadku.
<b>Zamówień publicznych i zlecenia zadań publicznych</b>	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.
<b>Odpowiedzialności</b>	Związane z obowiązkiem zapłaty kwot pieniężnych tytułem np. odszkodowań, odsetek karnych, kosztów procesowych.
<b>Realizacja programów współfinansowanych ze środków UE</b>	Związane z wystąpieniem nieprawidłowości przy wykorzystaniu środków z UE.
<b>Ryzyko dot. zasobów ludzkich</b>	
<b>Zarządzanie zasobami ludzkimi</b>	Związane z liczebnością i kompetencjami pracowników, szkoleniami, wprowadzaniem nowych zadań bez zabezpieczenia etatowego.
<b>BHP</b>	Związane ze zdrowiem pracowników i wypadkami przy pracy.
<b>Ryzyko działalności</b>	
<b>Regulacji wewnętrznych i zewnętrznych</b>	Związane z istnieniem i adekwatnością regulacji wewnętrznych i zewnętrznych.
<b>Organizacji i podejmowania decyzji</b>	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.
<b>Kontroli wewnętrznej</b>	Związane z funkcjonowaniem systemu kontroli wewnętrznej, np. ryzyko niedostatecznej kontroli, ryzyko nieskutecznych mechanizmów kontrolnych /działań zaradczych.
<b>Informacji</b>	Związane z jakością informacji, na podstawie których podejmowane są decyzje, np. ryzyko braku komunikacji wewnętrznej i zewnętrznej.
<b>Reputacji</b>	Związane z reputacją Jednostki, np. ryzyko negatywnych opinii.
<b>Ryzyko bezpieczeństwa informacji</b>	
<b>Ochrony informacji</b>	Związane z zapewnieniem bezpieczeństwa informacji przetwarzanych w

<b>(w tym danych osobowych) przetwarzanych w jednostce</b>	Urzędzie 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 Jednostki 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
<b>Ciągłości działania</b>	Związane np. z brakiem odpowiednich kompetencji do zapewnienia ciągłości działania zadań Jednostki.
<b>Ryzyko zewnętrzne</b>	
<b>Infrastruktury</b>	Związane z infrastrukturą, np. wyposażeniem, bazą lokalową, środkami transportu i środkami łączności.
<b>Środowiska prawnego</b>	Związane ze skomplikowaniem i zmianami prawa oraz niejednolitym orzecznictwem.