Załącznik nr 4
do zarządzenia Wójta Gminy Janowice Wielkie
z dnia…..

Procedura zarządzania ryzykiem w gminie oraz przykładowy arkusz zarządzania ryzykiem w Urzędzie Gminy

1. Wprowadzenie

1. Proces zarządzania ryzykiem jest procesem identyfikacji, oceny i przeciwdziałania występowania ryzyka. Obejmuje on:
1) możliwie jak najszybszą identyfikację ryzyka związanego z planowanym działaniem urzędu,
2) ocenę stopnia wpływu ryzyka na uzyskane wyniki lub cele urzędu,
3) zastosowanie odpowiednich środków kontroli ryzyka.

2. Kluczowym elementem polityki zarządczej jest określenie poziomu ryzyka tzw. „apetytu na ryzyko" tolerowanego przez Wójta Gminy i właścicieli procesów administracyjnych (pracowników). Struktura tego procesu obejmuje:
1) dokumentację dotyczącą zarządzania ryzykiem,
2) pełnione role i wykonywane zadania,
3) plany organizacyjne urzędu.

3. Celem procesu zarządzania ryzykiem jest określenie:
1) głównych celów dotyczących zarządzania ryzykiem oraz sposobu, w jaki łączą się one z celami Wójta Gminy,
2) struktury zarządzania ryzykiem, w tym danych o osobach ponoszących odpowiedzialność za działania kontrolne,
3) praktycznego sposobu zarządzania ryzykiem i minimalizowanie go.

4. Proces zarządzania zidentyfikowanymi ryzykami odnoszącymi się do zadań w gminie, dokonywany jest do końca II kwartału danego roku kalendarzowego.

5. Arkusz zarządzania ryzykiem jest integralnym elementem procedury, zawierającym ryzyka zidentyfikowane dla gminy. Pracownicy, do których przypisano poszczególne ryzyka, określają prawdopodobieństwa i ich wpływ na realizowane zadania zgodnie z metodą samooceny ryzyka.

6. Wypełnione arkusze zarządzania ryzykiem przekazuje się do Sekretarza Gminy.

7. Sekretarz Gminy opracowuje i przekazuje Wójtowi Gminy raport o zidentyfikowanych ryzykach.

2. Słownik pojęć

Pojęcie	**Opis**
Ryzyko	prawdopodobieństwo zaistnienia negatywnego zdarzenie, redukującego szansę Wójta Gminy na osiągnięcie celów

Wpływ	wielkość zaburzeń uniemożliwiających urzędowi skuteczne funkcjonowanie
Apetyt na ryzyko	maksymalny poziom iloczynu ryzyka i wpływu, jaki Wójt gotowy jest tolerować, zanim uzna, że konieczna jest interwencja.
Zarządzanie ryzykiem	proces, którego celem jest identyfikacja ryzyka, oszacowanie wpływu i podjęcie działań w przypadku ustalenia, że apetyt na ryzyko został przekroczony
Samoocena ryzyka	metoda zarządzania ryzykiem polegająca na dokonywaniu pomiarów ryzyka i wpływu przez pracowników i ich przełożonych
Reakcja na ryzyko	podjęcie działań w wyniku stwierdzenia ryzyka przekraczającego apetyt, polegające na: - przeniesieniu ryzyka na inny podmiot, - tolerowaniu podwyższonego ryzyka, - wdrożeniu nowych mechanizmów redukujących ryzyko, - wycofaniu się z działalności w danym obszarze.

3. Poziomy ryzyka i wpływu

Ustala się 4 poziomy ryzyka, spośród których jeden jest przypisywany przez pracownika dokonującego oceny ryzyka:

Ryzyko	**Opis**
Krytyczne (K)	ryzyko może zmaterializować się w czasie krótszym niż kwartał ; prawdopodobieństwo wynosi > 80%
Wysokie (W)	ryzyko może zmaterializować się w okresie do pół roku; prawdopodobieństwo wynosi od 41-80%
Średnie (S)	ryzyko może zmaterializować się w ciągu najbliższego roku; prawdopodobieństwo wynosi od 20-40%
Niskie (N)	ryzyko może zmaterializować się w wyjątkowych przypadkach

Ustala się 4 poziomy wpływu, spośród których jeden jest przypisywany przez pracownika dokonującego oceny ryzyka:

Wpływ	**Opis**
Krytyczny (K)	poważne problemy z realizacją zadań; poważne problemy z jakością wykonywanej pracy; bardzo duży wpływ na koszty, zasoby lub reputację
Wysoki (W)	problemy z realizacją zadań; problemy z jakością wykonywanej pracy; duży wpływ na koszty, zasoby, reputację

Średni(S)	obniżenie jakości realizowanych zadań; mały wpływ na koszty, zasoby lub reputację
Niski (N)	nieznaczne obniżenie jakości realizowanych zadań; minimalny wpływ na koszty, zasoby, reputację

Dla procesów realizowanych w gminie dopuszcza się niski i średni poziom ryzyka. Może on być modyfikowany przez właścicieli poszczególnych procesów (pracowników).

Krytyczny	**W**	**W**	**K**	**K**
Wysoki	s	**W**	**W**	**K**
Średni	N	s	**W**	**W**
Niski	N	N	s	**W**
	Niskie	*Średnie*	*Wysokie*	*Krytyczne*
	Prawdopodobieństwo			

W przypadku, gdy dla danego ryzyka określony zostanie poziom krytyczny lub wysoki, zgłaszający pracownik omawia z Sekretarzem Gminy, jakie dodatkowe mechanizmy kontrolne mogłyby zredukować to ryzyko do niższego poziomu. Jeśli rozwiązanie problemu nie jest możliwe w ramach środków, jakimi dysponuje dana komórka organizacyjna, ostateczną decyzję w sprawie rozwiązania problemu podejmuje Wójt Gminy.

Katalog mechanizmów kontrolnych redukujących ryzyko

1. Regulacje zewnętrzne i wewnętrzne: ustawy, umowy międzynarodowe, rozporządzenia, uchwały, zarządzenia, plany, polityki, wytyczne, instrukcje, procedury, standardy przyjęte, jako obowiązujące w jednostce, metodyki, umowy cywilno-prawne.

2. Opisy funkcji i stanowisk pracy, zakresy czynności i obowiązków. Dokumenty określające zakres:

1) kompetencji i odpowiedzialności,
2) upoważnień i pełnomocnictw,
3) zastępstw, sprawowanego nadzoru,
4) wykonywanej kontroli wewnętrznej.

3. System obiegu informacji i raportowania:

1) zapewnienie dostępu do informacji w terminie i zakresie właściwym do wykonywania zadań,
2) raportowanie wykonania zadań wobec przełożonych,
3) porównywanie osiągniętych wyników z zamierzonym celami.

4. Uzgadnianie stanowisk, kierunków działań:

1) zasięganie opinii zainteresowanych jednostek, wewnętrznych i zewnętrznych w celu wypracowania wspólnej strategii działania,
2) uzgadnianie aktów prawnych regulacji wewnętrznych i zewnętrznych.

5. Uzgadnianie danych. Porównywanie zgodności danych zawartych w różnych dokumentach lub systemach informatycznych.
6. Zasada komisyjności „czworga oczu”, „na dwie ręce":

1) wykonywanie czynności przy współudziale, co najmniej dwóch osób,
2) komisje inwentaryzacyjne, spisowe,
3) zespoły kontrolne,
4) rejestracja i autoryzacja transakcji.

7. System limitów i ograniczeń:

1) ograniczenia czasowe dla: rejestracji operacji, załatwiania spraw, udzielania odpowiedzi,
2) ustawowe ograniczenie czasowe np. spłaty zaciągniętych zobowiązań,
3) ograniczenia finansowe przy podejmowaniu decyzji, zawieraniu transakcji, zaangażowaniu wobec stron trzecich,

8. Analiza kontrahentów/uczestników rynku, w tym sprawdzanie wiarygodności:

1) finansowej podmiotów zewnętrznych,
2) uczestników przetargu,
3) dostawców towarów i usług. 9. Kontrola dostępu oraz zabezpieczenia teleinformatyczne:

1) zakazy i ograniczenia dostępu fizycznego osób do: pomieszczeń, systemów i danych, internetu, zagranicznych i zamiejscowych rozmów telefonicznych, szyfrowania, podpisu elektronicznego,

2) możliwości nagrywania rozmów telefonicznych.

10. Inwentaryzacja i spis z natury:

1) porównywanie zgodności stanu fizycznego/rzeczywistego zasobów ze stanem zapisów w księgach rachunkowych, rejestrach,

2) inwentaryzacja rzeczowych składników majątkowy,

3) dzienne uzgadnianie stanu wartości.

11. Zabezpieczenia fizyczne:

1) ochrona fizyczna zasobów jednostki rzeczowych, osobowych, w tym zabezpieczenie gotówki, papierów wartościowych, obiektów,

2) dokumentów zakwalifikowanych do informacji niejawnych w kancelarii tajnej,

3) zabezpieczenie fizyczne serwerów przed dostępem osób nieuprawnionych, zalaniem lub pożarem.

12. Kopie zapasowe, na wypadek utraty oryginalnych danych, zapasowe generatory prądotwórcze, na wypadek awarii zasilania.

13. Plany zarządzania kryzysem:

1) plany awaryjno- odtworzeniowe, odtworzenie infrastruktury krytycznej, obszarów uznanych za krytyczne,

2) plany działania procesów, podtrzymywanie działania procesów, świadczenia usług na akceptowalnym poziomie podczas kryzysu,

3) plany ciągłości działania, systemowe podejście do utrzymania funkcjonowania działalności przed - w czasie - i po katastrofie,

4) testowanie opracowanych planów, ćwiczenie zdolności zespołów do praktycznego wypełniania zaplanowanych działań oraz sprawdzanie aktualności planów w zmieniającym się otoczeniu i nowych rodzajach ryzyka.

14. Rezerwy finansowe, na pokrycie strat związanych z niewypłacalnością kontrahentów koniecznością pokrycia kwot gwarancji i poręczeń.

15. Ubezpieczenia mienia od zdarzeń losowych, kradzieży.

16. Usługi zewnętrzne, dzielenie się ryzykiem, które obciążałoby jednostkę w sytuacji gdyby zadania były wykonywane przy wykorzystaniu zasobów własnych.

17. Audyt i kontrola:

1) kontrole prawidłowości i terminowości realizacji zadań,

2) kontrole czasu pracy i ruchu osobowego,

3) kontrole realizacji reakcji na ryzyko, poprawności i terminowości,

4) kontrola realizacji zaleceń pokontrolnych,

5) ocena skuteczności kontroli funkcjonalnej,

6) ocena systemu zarządzania ryzykiem, kontroli wewnętrznej i ładu organizacyjnego.

18. Analiza mierników: wydajności, efektywności, osób i urządzeń, awaryjności urządzeń i utraconego czasu pracy, BHP, obrażeń i odszkodowań oraz absencji.

19. Testowanie nowych rozwiązań, projektów, systemów informatycznych przed ich wdrożeniem.

20. Zarządzanie bezpieczeństwem informacji, szkolenie pracowników.

21. Analiza informacji przekazywanych od pracowników oraz pozyskiwanych od stron zewnętrznych: mieszkańców, klientów, dostawców, odbiorców usług, ekspertów, audytorów i konsultantów.

Podana powyżej lista mechanizmów kontrolnych stanowi przykładowy wzór do uzupełnienia i dostosowania do specyfiki jednostki organizacyjnej.