ZARZĄDZENIE Nr 4/24
Dyrektora Zespołu Parków Krajobrazowych
Województw Śląskiego
z dnia 14 marca 2024 roku

W sprawie: aktualizacji procedur zarządzania ryzykiem w Zespole Parków Krajobrazowych Województwa Śląskiego

Na podstawie art. 69 ust. 1 pkt. 3 Ustawy z dnia 27 czerwca 2009 r. o finansach publicznych (Dz. U. z 2013 roku Nr 885, poz. 1240 z późn. zm.) oraz Komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Min. Fin. z 2009 roku Nr 15, poz. 84) oraz Komunikatu 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. Min. Fin. z 2012 roku poz. 56) oraz wytycznych Urzędu Marszałkowskiego Województwa Śląskiego.

zarządzam, co następuje:

§ 1

W Zespole Parków Krajobrazowych Województwa Śląskiego obowiązuje Procedura zarządzania ryzykiem, stanowiąca załącznik do niniejszego Zarządzenia.

§ 2

Wykonanie Zarządzenia powierzam Zespołowi ds. kontroli zarządczej.

§ 3

Nadzór nad realizacją Zarządzenia powierzam Przewodniczącemu Zespołu ds. kontroli zarządczej.

§ 4

Traci moc Zarządzenie Dyrektora nr 15/22 z dnia 2 sierpnia 2022r. w sprawie aktualizacji procedur zarządzania ryzykiem w Zespole Parków Krajobrazowych Województwa Śląskiego.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
Do Zarządzenia Nr 4/24
Dyrektora ZPKWŚ
z dnia 14 marca 2024r.

Procedura zarządzania ryzykiem
w Zespole Parków Krajobrazowych
Województwa Śląskiego

§ 1
[Cel i zakres procedury]

1. Celem procedury jest zapewnienie jednolitego sposobu zarządzania ryzykiem w Zespole Parków Krajobrazowych Województwa Śląskiego poprzez:
   1) zapewnienie, iż wszystkie istotne szanse i zagrożenia odnoszące się do realizacji zadań, procesów, celów, aktywów są identyfikowane i analizowane na bieżąco,
   2) zapewnienie porównywalności wyników oceny ryzyka w różnych obszarach działalności Zespołu,
   3) w miarę potrzeb opracowywanie i wdrażanie odpowiednich planów postępowania z ryzykiem,
   4) zapewnienie skutecznej komunikacji pomiędzy komórkami organizacyjnymi Zespołu oraz komunikacji z kierownictwem Zespołu w zakresie poszczególnych ryzyk,
   5) określenie odpowiedzialności za zarzadzanie poszczególnymi ryzykami.
2. Procedura opisuje:
   1) przebieg procesy zarządzania ryzykiem w tym metodykę oceny ryzyka,
   2) role, odpowiedzialności, obowiązki i uprawnienia w zakresie zarządzania ryzykiem,
   3) komunikowanie i informowanie o ryzyku,
   4) zasady dokumentowania zarzadzania ryzykiem.
3. Zarządzanie ryzykiem w Zespole Parków Krajobrazowych Województwa Śląskiego to proces identyfikacji, analizy, oceny, monitorowania i reagowania na ryzyko, zmierzający do zapewnienia, że zdefiniowane i określone cele i zadania Zespołu zostaną zrealizowane przez komórki organizacyjne.
4. Użyte w niniejszym dokumencie pojęcia mają następujące znaczenie:
   1) **Zespół** – Zespół Parków Krajobrazowych Województwa Śląskiego.
   2) **Dyrektor** – Dyrektor Zespołu Parków Krajobrazowych Województwa Śląskiego,
   3) **komórka organizacyjna** – Dział Biura Zespołu Parków,
   4) **kierownik komórki organizacyjnej Zespołu** – osoba kierująca komórką organizacyjną,
   5) **cele priorytetowe Województwa** – najważniejsze cele operacyjne Zespołu włączone do aktualnie obowiązującej strategii rozwoju Województwa, wybrane przez Marszałka jako najważniejsze cele Województwa do realizacji na dany rok,

6) **cele operacyjne** – wyznaczone do realizacji na dany rok cele komórki organizacyjnej Zespołu,
7) **aktywa** – rozumiane jako aktywa bezpieczeństwa informacji, np. sprzęt, oprogramowanie, sieć, struktura organizacyjne,
8) **bezpieczeństwo informacji** – zachowanie poufności, integralność, dostępność i rozliczalność informacji,
9) **działanie** – obszar aktywności taki jak zadanie, proces, cel, projekt, zmiana itp.,
10) **incydent** – odnotowane zdarzenie mogące doprowadzić do materializacji ryzyka (materializacja przyczyny ryzyka),
11) **ryzyko** – możliwość wystąpienia zdarzenia mającego negatywny wpływ na realizację założonych celów i zadań lub uniemożliwiającego realizację celów i zadań,
12) **mechanizmy kontroli/zabezpieczenia** – środki, które modyfikują ryzyko, w szczególności działania, procedury, instrukcje i zasady służące zapewnieniu realizacji celów, ograniczeniu wystąpienia ryzyka nieosiągnięcia celów lub zmniejszeniu jego negatywnych skutków, a także środki techniczne i organizacyjne zapewniające ochronę informacji,
13) **reakcja na ryzyko** - dodatkowy mechanizm lub grupa mechanizmów kontrolnych, mających na celu zmniejszenie poziomu ryzyka rezydualnego,
14) **zarządzanie ryzykiem** – proces identyfikacji, analizy, oceny, monitorowania i reagowania na ryzyko, zmierzający do zapewnienia, że wyznaczone cele i zadania zostaną zrealizowane,
15) **właściciel ryzyka** – osoba odpowiedzialna za zapewnienie, że ryzyko jest zarządzane i monitorowane oraz posiadająca uprawnienia wystarczające do zapewnienia efektywnego zarządzania ryzykiem, np. Dyrektor dla ryzyk priorytetowych, osoba kierująca Działem dla ryzyk operacyjnych/merytorycznych, bezpośredni przełożony,
16) **opiekun ryzyka** – wyznaczony przez właściciela ryzyka pracownik, do którego zadań należy w szczególności wspieranie właściciela ryzyka w zakresie zarzadzania konkretnym ryzykiem oraz zbieranie informacji na temat ryzyka, którego jest opiekunem,
17) **ocena ryzyka** – proces identyfikacji, analizy i ewaluacja ryzyka,
18) **wewnętrzny rejestr ryzyk** – zbiór informacji dotyczących zidentyfikowanych ryzyk komórek organizacyjnych, prowadzony w formie papierowej i cyfrowej,
19) **zbiorczy rejestr ryzyk Zespołu** – zbiór informacji dotyczących zidentyfikowanych ryzyk Zespołu, prowadzony w formie papierowej i cyfrowej.

§ 2

1. Za zarządzanie ryzykiem w komórce organizacyjnej odpowiada właściciel ryzyka.
2. Proces zarządzania ryzykiem obejmuje następujące etapy:
   1) ustalenie kontekstu,
   2) ocenę ryzyka (w tym: identyfikacja, analiza, ewaluacja ryzyka),

3) wdrożenie planu postępowania z ryzykiem nieakceptowalnym (reakcja na ryzyko),
4) monitorowanie ryzyka,
5) dokumentowanie zarządzania ryzykiem, tj. wyznaczenie celów i ryzyk, wewnętrzny i zewnętrzny rejestr ryzyk oraz ich monitorowanie oraz raportowanie ryzyka.

3. W toku procesu zarządzania ryzykiem należy brać pod uwagę w szczególności:
   1) specyfikę realizowanego działania (zadania, procesu, celu), rodzaj aktywów,
   2) zagrożenia/szanse związane z realizowaniem działań oraz zarządzaniem aktywami, ze wskazaniem ich źródeł i skutków zarówno zewnętrznych, jak i wewnętrznych,
   3) rodzaj ryzyka (operacyjne, bezpieczeństwa informacji, przetwarzania danych osobowych, korupcyjne).

§ 3
[Ustalenie kontekstu]

1. Ustalenie kontekstu polega na rozpoznaniu otoczenia mającego wpływ na realizowane działanie lub na aktywa.
2. Analizie podlega kontekst:
   1) wewnętrzny – związany z wewnętrznymi uwarunkowaniami organizacji, środowiskiem pracy, w którym realizowane jest działanie, posiadanymi zasobami, organizacją pracy, funkcjonujący system zarządzania, w tym system zarządzania bezpieczeństwem informacji, ochrony danych osobowych itp.,
   2) zewnętrzny – związany z otoczeniem zewnętrznym, np. przepisami prawa, uwarunkowaniami środowiskowymi, stronami zainteresowanymi, w tym jednostkami organizacyjnymi itp.
3. Analiza kontekstu wewnętrznego i zewnętrznego stanowi podstawę do dokonania oceny ryzyka.
4. **Nie jest wymagane dokumentowanie kontekstu działania.**

§ 4
[Identyfikacja ryzyka]

1. Celem identyfikacji ryzyka jest zgromadzenie informacji na temat istniejących ryzyk.
2. Efektem identyfikacji ryzyka jest lista, zawierająca informacje o zidentyfikowanych ryzykach.
3. Identyfikacja ryzyka polega na ustaleniu (wyszukaniu, rozpoznaniu i opisaniu) występujących lub możliwych do wystąpienia zdarzeń, zjawisk, czynników, sytuacji itp., zagrażających lub sprzyjających realizacji działań lub aktywom.

4. Zdarzenia, zjawiska, czynniki, sytuacje mogą odnosić się do takich obszarów jak: infrastruktura, informatyka, zasoby ludzkie, finanse/budżet, prawo, regulacje wewnętrzne, umowy, zarządzanie, organizacja, komunikacja, informacja, współpraca, polityka, klient zewnętrzny i inne.
5. Podczas identyfikacji ryzyka kierownik komórki organizacyjnej pełniący rolę właściciela ryzyka powinien dokonać analizy zadań, procesów, celów i aktywów, za których realizację odpowiada lub którymi zarządza.
6. W proces identyfikacji ryzyka włączeni są wszyscy realizujący cel pracownicy komórki organizacyjnej oraz osoba odpowiedzialna za realizację działania lub odpowiedzialni za aktywa (w szczególności kierownik komórki organizacyjnej / bezpośredni przełożony).
7. Każdy pracownik komórki organizacyjnej zobligowany jest do pisemnego informowania kierownika komórki organizacyjnej pełniącego rolę Właściciela ryzyka o wszystkich istotnych ryzykach lub zdarzeniach przez niego zidentyfikowanych w toku realizacji zadań.
8. Przełożony umożliwi pracownikom swobodną identyfikację ryzyk w szczególności przez zapewnienie o braku jakichkolwiek form reperkusji związanych ze zidentyfikowaniem ryzyka przez pracowników.
9. Kierownik komórki organizacyjnej / bezpośredni przełożony – właściciel ryzyka, po przeanalizowaniu zgłoszenia, decyduje o konieczności umieszczeniu ryzyka w wewnętrznym rejestrze ryzyk.
10. Zadaniem właściciela ryzyka jest odpowiedź na pytanie jakie występujące lub potencjalne negatywne zdarzenia mogą mieć wpływ na realizację zdefiniowanego celu bądź zadania komórki organizacyjnej.
11. Właściciel ryzyka identyfikuje, analizuje i ocenia zidentyfikowane ryzyka samodzielnie lub współpracując z pozostałymi pracownikami komórki organizacyjnej. Przy analizie i ocenie ryzyk należy kierować się w szczególności wiedzą specjalistyczną osób identyfikujących ryzyka, doświadczeniami z przeszłych zdarzeń, prognozami na przyszłość, ustaleniami z narad, wniosków pokontrolnych (kontrola funkcjonalna i instytucjonalna) a także każdą inna wiedzą na temat potencjalnych wydarzeń, mogących mieć wpływ na analizowany obszar.
12. Należy unikać określania ryzykiem sytuacji, czynników, zdarzeń, które nie mają wpływu na działanie lub aktywa.
13. Nie można określić minimalnej i maksymalnej liczby ryzyk, którą należy zidentyfikować. Ważne jest, aby zidentyfikowane ryzyko w rzeczywisty sposób opisywały zagrożenia, które mogą wpłynąć na działanie. Należy jednak pamiętać, że określenie zbyt dużej ilości ryzyk może powodować problemy w zarządzaniu nimi.
14. W wyniku identyfikacji ryzyk w komórce organizacyjnej powstaje wewnętrzny rejestr ryzyk mogących mieć negatywny wpływ na działanie.
15. W przypadku zmian organizacyjnych w Zespole kierownicy komórek organizacyjnych, których zmiany dotyczą, dokonują weryfikacji lub ponownej identyfikacji i analizy ryzyk do wyznaczonych celów wprowadzając zmiany w wewnętrznym rejestrze ryzyk.

16. W przypadku zidentyfikowania lub wystąpienia ryzyk obejmujących realizację celów w skali całego Zespołu lub znacznej jego części właściciele ryzyk podejmują wspólne działania mające na celu wprowadzenie jednolitych mechanizmów kontroli dla ryzyk.
17. Ryzyka mogą być identyfikowane w ramach poszczególnych działań oraz w odniesieniu do aktywów:
    1) w przypadku rozpoczęcia realizacji działania lub zidentyfikowania nowych aktywów,
    2) w toku bieżącej działalności,
    3) podczas monitorowania ryzyk,
    4) każdorazowo w przypadku materializacji ryzyka,
    5) każdorazowo w przypadku wystąpienia istotnej zmiany kontekstu wewnętrznego lub zewnętrznego, pozostającej w związku ze zidentyfikowanymi ryzykami,
    6) w ramach przeglądu systemu.
18. Ustala się następujące **obszary ryzyk** stosowanych jako narzędzie pomocnicze przy identyfikacji ryzyk. Lista nie stanowi zbioru zamkniętego i może być rozbudowana o kolejne obszary charakterystyczne dla danego celu/działania:
    1) infrastruktura,
    2) informatyka,
    3) bezpieczeństwo informacji,
    4) bezpieczeństwo zasobów,
    5) zasoby ludzkie,
    6) finanse/budżet,
    7) prawo,
    8) regulacje wewnętrzne,
    9) realizacja zadań na podstawie zawartych umów,
    10) zarządzanie,
    11) organizacja,
    12) komunikacja,
    13) informacja,
    14) współpraca,
    15) polityka,
    16) klient zewnętrzny,
    17) inne.

§ 5

[Analiza ryzyka informacje ogólne]

1. **Celem analizy ryzyka** jest dokonanie szczegółowej analizy każdego zidentyfikowanego ryzyka, polegające na dokonaniu dogłębnej analizy informacji na temat ryzyka, jego charakteru i elementów, co umożliwi wyznaczenie poziomu ryzyka w dalszym etapie procesu.
2. **Efektem analizy ryzyka** jest rejestr ryzyk ze wskazaniem kluczowych elementów opisujących ryzyko – dokonanie oceny prawdopodobieństwa i skutków, dokonanie

identyfikacji i oceny skuteczności mechanizmów kontroli/zabezpieczeń oraz uzyskanie wartości każdego zidentyfikowanego ryzyka stanowiącej podstawę do jego ewaluacji.

3. **Analiza ryzyka** dokonywana jest każdorazowo po identyfikacji nowego ryzyka lub w ramach monitorowania ryzyk.
4. **Podczas analizy można wykorzystać takie techniki pracy i źródła wiedzy jak:**
   1) narady,
   2) wywiady,
   3) warsztaty,
   4) ankiety,
   5) burze mózgów,
   6) bazy incydentów,
   7) dokumentację audytową lub procesową,
   8) raporty i statystyki incydentów,
   9) inne raporty,
   10) prognozy na przyszłość.

   Analizując ryzyko należy również wziąć pod uwagę kontekst Zespołu.
5. Kierownicy komórek organizacyjnych pełniący rolę Właściciela ryzyka mogą dokonywać analizy osobiście bądź przy współpracy z wyznaczonymi pracownikami, tj. Opiekunami ryzyka.
6. Wszystkie analizy wprowadzane są do rejestru ryzyka.
7. **Etapy analizy ryzyka:**
   1) ustalenie właściciela ryzyka,
   2) informowanie o ryzyku,
   3) ustalenie przyczyn i skutków ryzyka,
   4) wskazanie funkcjonujących mechanizmów kontroli dla analizowanego ryzyka,
8. Wszystkie ryzyka muszą mieć swojego **określonego imiennie właściciela**, który jest odpowiedzialny za zapewnienie, że ryzyko jest zarządzane i monitorowane. **Właściciel ryzyka powinien mieć uprawnienia wystarczające do zapewnienia efektywnego zarządzania ryzykiem (np. kierownik komórki organizacyjnej).** W przypadku zidentyfikowania ryzyka wykraczającego poza kompetencje kierownika komórki organizacyjnej wiedza na temat tego ryzyka przekazywana jest do osoby, która może nim skutecznie zarządzać.
9. W przypadku zidentyfikowania ryzyka wykraczającego poza kompetencje kierownika komórki organizacyjnej lub odnoszącego się do działania realizowanego przez inną komórkę organizacyjną wiedza na temat tego ryzyka jest przekazana pisemnie do osoby, która może nim skutecznie zarządzać. Analogiczna zasadę stosuje się do właścicieli ryzyk niebędących kierownikami komórek organizacyjnych.
10. Informowanie o ryzyku ma na celu osiągnięcie porozumienia, co do sposobu zarządzania ryzykiem poprzez wielostronną wymianę informacji pomiędzy osobami bezpośrednio zaangażowanymi w jego zarządzanie oraz innymi uczestnikami procesu

zarządzania ryzyk w Zespole. Skuteczna komunikacja pomaga w podejmowaniu decyzji dotyczących ryzyka.

11. Ustalając przyczyny i skutki ryzyka należy przeanalizować między innymi:

1) doświadczenia z przeszłych zdarzeń np. wyniki kontroli, obszary których dotyczyły skargi, sprawozdania, raporty i analizy okresowe z realizacji zadań, obserwacje, tendencje, absencje,
2) prognozy na przyszłość, symulacje,
3) czynniki zewnętrzne i wewnętrzne, które mają wpływ na realizację celów i wystąpienie ryzyka (kontekst działania),
4) podatność na ryzyka.

12. Dla każdego ryzyka należy wskazać mechanizmy kontroli/zabezpieczenia stosowane na dzień przeprowadzenia analizy oraz dokonać oceny ich skuteczności w kontekście minimalizacji poziomu analizowanego ryzyka.
13. Wskazanie funkcjonujących mechanizmów kontroli/zabezpieczenia może również przyczynić się do zidentyfikowania mechanizmów niepotrzebnych, zbyt kosztownych lub nieuzasadnionych dla sprawnej realizacji działania, a także mechanizmów kontroli/zabezpieczeń zbyt słabych i wymagających poprawy.

14. Wskazanie mechanizmów kontroli/zabezpieczeń ma na celu:

1) minimalizacja prawdopodobieństwa i skutków ryzyk,
2) sprawdzenie funkcjonujących mechanizmów kontrolnych,
3) właściwa realizacja zadań,
4) przejrzystość wykonywanych czynności i podejmowanych decyzji.

Przykładowe mechanizmy kontroli:

1) przepisy prawa,
2) instrukcje,
3) procedury,
4) wytyczne,
5) listy kontrolne (checklisty)
6) dobre praktyki (sprawdzone rozwiązania),
7) zasada dwóch par oczu,
8) schematy,
9) wzory dokumentów,
10) punkty kontrolne w obiegu dokumentów (zatwierdzenia),
11) zamykana szafa, biurko,
12) zasady zastępstw,
13) okresowe sprawdzanie przestrzegania przyjętych zasad,
14) poufność haseł dostępu i ich okresowe zmiany,
15) kopie zapasowe,
16) ubezpieczenia.

4) Dla ułatwienia analizy można wypisać funkcjonujące mechanizmy kontrolne. Pozwoli to dokładniej ocenić ich wpływ na obniżenie prawdopodobieństwa i skutków ryzyka.

15. Dla każdego zidentyfikowanego ryzyka należy sporządzić jego opis:
    1) określić działanie lub aktywo, w którym zidentyfikowano ryzyko,
    2) wskazać rodzaj ryzyka,
    3) wskazać charakter ryzyka poprzez zdefiniowanie czy ryzyko stanowi zagrożenie, czy szanse dla Zespołu,
    4) wskazać Właściciela ryzyka,
    5) wskazać potencjalne przyczyny zewnętrzne i/lub wewnętrzne powodujące ryzyko oraz skutki wystąpienia ryzyka. Ustalając przyczyny i skutki ryzyka należy przeanalizować m. in. Czy w liście ryzyk, o której mowa w § 4 znajdują się zdarzenia będące przyczynami lub skutkami wystąpienia innych ryzyk tworzące ciąg logiczny:
    Z powodu……(przyczyna)istnieje ***ryzyko****……,które spowoduje……(skutek)*,
    6)w sytuacji, gdy zidentyfikowane zdarzenie (ryzyko) może być przyczyną lub skutkiem innego ryzyka należy zakwalifikować je odpowiednio do przyczyn lub skutków właściwego ryzyka. Ostatecznie wszystkie ryzyka wraz z przyczynami i skutkami powinny tworzyć ww. ciąg logiczny.

§ 6

[Analiza ryzyka polegająca na wyznaczeniu poziomu prawdopodobieństwa ryzyka]

1. Pierwszym kryterium analizy każdego z ryzyk jest prawdopodobieństwo wystąpienia ryzyka na dzień przeprowadzania analizy po zastosowaniu działań określonych jako mechanizmy kontroli/zabezpieczenia.
2. Przyjęte pomocnicze skale prawdopodobieństwa wystąpienia ryzyka wskazane zostały poniżej. Należy wziąć pod uwagę zgłoszone incydenty.

Prawdopodobieństwo		**Opis**
1	**Znikome**	zagrożenie jest mało realne, aby mogło wystąpić (nie miało nigdy miejsca), zabezpieczenia: są skuteczne i monitorowane, dane historyczne (incydenty bezpieczeństwa i audyty wewnętrzne): nie występuje, podatności: brak.
2	**Mało prawdopodobne**	zagrożenie nie miało miejsca w przeszłości i istnieje niewielkie prawdopodobieństwo, że wystąpi w przyszłości, zabezpieczenia: są skuteczne, dane historyczne (incydenty bezpieczeństwa i audyty wewnętrzne): bardzo nieliczne wystąpienia (1-2), podatności: bardzo nieliczne.

3	**Prawdopodobne**	zagrożenie występuje w innych organizacjach i może wystąpić w Zespole (jak w innej jednostce o podobnym charakterze), zabezpieczenia: są, ale nieskuteczne, dane historyczne (incydenty bezpieczeństwa i audyty wewnętrzne): nieliczne wystąpienia (3-5), podatności: nieliczne.
4	**Bardzo prawdopodobne**	zagrożenie może wystąpić, gdyż miało miejsce w przeszłości i należy sądzić, że wystąpi co najmniej raz w ciągu roku, zabezpieczenia: tylko dobre praktyki, dane historyczne (incydenty bezpieczeństwa i audyty wewnętrzne):wystąpienia (6-10), podatności: liczne.
5	**Prawie pewne**	zagrożenie jest bardzo realne i może wystąpić w każdej chwili lub kilkakrotnie w ciągu roku, zabezpieczenia: brak dane historyczne (incydenty bezpieczeństwa i audyty wewnętrzne): liczne wystąpienia (powyżej 10) podatności: bardzo liczne..

§ 7
[Analiza ryzyka polegająca na wskazaniu skutków wystąpienia ryzyka]

1. Dokonując analizy możliwych skutków danego ryzyka należy brać pod uwagę najbardziej prawdopodobne konsekwencje spowodowane zmaterializowaniem się ryzyka z uwzględnieniem stosownych działań określonych w mechanizmach kontroli/zabezpieczeniach.
2. Dla poszczególnych rodzajów ryzyka ustalenie i ocena skutków powinna być proporcjonalna, z zastosowaniem odpowiednich czynników, np. dla ryzyk na poziomie działań strategicznych nie powinno się opisywać i oceniać szczegółowych skutków związanych z działaniami operacyjnymi na poziomie jednej komórki organizacyjnej.
3. Analiza skutków dotyczy głównie wpływu ryzyka na konkretne działanie lub aktywo, ale może także odnosić się do wpływu ryzyka na inne działania lub obszary funkcjonowania Zespołu.
4. Podczas dokonywania oceny należy ocenić każdy rodzaj skutku.
5. Ryzyka poszczególnych rodzajów, np. ryzyka korupcyjne są dodatkowo obarczone innymi skutkami, w szczególności wizerunkowymi i prawnymi.
6. Należy zawsze brać pod uwagę wystąpienie kilku zagrożeń w tym samym czasie, a także zmaterializowanie się nowego zagrożenia po wystąpieniu innego zagrożenia (efekt domina).
7. Pomocnicze skale oceny skutków materializacji poszczególnych rodzajów ryzyka przedstawia poniższa tabela:

Tabela 1.

Skutki *		**Realizacja działania**	**Ciągłość działalności**	**Wizerunek**	**Bezpieczeństwo informacji**	**Naruszenie prawa i procedur**	**Korupcja**
1	Nieznaczące	Brak opóźnienia w realizacji działania	Brak zakłóceń pracy	Brak wpływu na postrzeganie jednostki, brak informacji w mediach	Krótkotrwałe i nieznaczne zakłócenia w dostępie do informacji w danym procesie	Brak konsekwencji prawnych, w tym karno-skarbowych	Brak złamania zasad przeciwdziałania korupcji
2	Niewielkie	Krótkie opóźnienia bez wpływu na działanie	Niewielkie utrudnienia w pracy	Niewielki wpływ na postrzeganie jednostki przez otoczenie zewnętrzne oraz pracowników, pojedyncze informacje w mediach lokalnych	Niewielkie zakłócenia w dostępie do informacji w danym procesie oraz niskie prawdopodobieństwo udzielenia informacji osobom nieuprawnionym	Naruszenie procedur wewnętrznych nieskutkujące odpowiedzialnością służbową	Złamanie wewnętrznych regulacji, konieczność prowadzenia postępowania wyjaśniającego
3	Istotne	Opóźnienia mogące mieć wpływ na realizację działania	Utrudnienia mające wpływ na ciągłość działania	Zauważalne niezadowolenie pracowników oraz otoczenia zewnętrznego, informacje w mediach lokalnych i regionalnych	Zakłócenia w dostępie do informacji we właściwym czasie wraz z prawdopodobieństwem udzielenia informacji osobom nieuprawnionym	Naruszenie procedur wewnętrznych mogące doprowadzić do negatywnych wyników kontroli, naruszenie prawa bez konsekwencji	Złamanie wewnętrznych regulacji i naruszenie podstawowych obowiązków pracownika, uruchomienie procedury dyscyplinarnej, możliwa odpowiedzialność cywilna pracownika
4	Duże	Opóźnienia mające wpływ na realizacje działania	Odczuwalny wpływ na ciągłość działania	Duże niezadowolenie pracowników oraz otoczenia zewnętrznego, pojedyncze informacje w mediach ogólnokrajowych	Poważne zakłócenia w dostępie do informacji we właściwym czasie i z dużym prawdopodobieństwem udzielenia informacji osobom nieuprawnionym. Niskie prawdopodobieństwo utraty lub zmiany informacji w sposób nieautoryzowany	Rażące naruszenie procedur wewnętrznych, naruszenie prawa prowadzące do umiarkowanych konsekwencji, w tym naruszenia dyscypliny finansów publicznych (niski stopień szkodliwości)	Pozew skierowany przeciwko pracownikowi, odpowiedzialność cywilna lub karna pracownika (zwiększona szkodliwość społeczna)

5	Bardzo duże	Realizacja działania jest zagrożona, może zostać całkowicie wstrzymana	Bardzo duże, długotrwałe utrudnienia w ciągłości działania	Katastrofalny wpływ wizerunkowy, informacje w mediach ogólnokrajowych i międzynarodowych	Brak dostępu do informacji we właściwym czasie	Rażące naruszenie prawa zagrożone odpowiedzialnością karną, skarbową lub za naruszenie dyscypliny finansów publicznych (wysoki stopień szkodliwości)	Pozew skierowany przeciwko pracownikowi, odpowiedzialność cywilna lub karna pracownika (zwiększona szkodliwość społeczna)

*Należy ocenić równocześnie wszystkie rodzaje skutków. Podczas oceny należy brać pod uwagę **najbardziej prawdopodobny** do wystąpienia skutek. Jeżeli z ryzykiem nie wiąże się dany rodzaj skutku należy wybrać wartość jeden.

Tabela 2.

<table>
<tr><th colspan="2">Skutki*</th><th>Naruszenie praw lub wolności osób fizycznych</th><th>Dodatkowe informacje</th></tr>
<tr><td>1</td><td>Nieznaczące</td><td>Nieznaczący lub niezauważalny wpływ na prawa lub wolności osób. Brak realnych możliwości zaszkodzenia osobie</td><td rowspan="4">Oceniając skutki naruszenia praw lub wolności osób fizycznych należy rozpatrywać je z punktu widzenia osoby, której dane dotyczą a nie z punktu widzenia administratora danych. Ryzyka z punktu widzenia administratora danych co do zasady powinny być oceniane w pozostałych obszarach, np. bezpieczeństwa informacji.

Zgodnie z motywem 75 RODO:
Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

1) jeżeli przetwarzanie może poskutkować dyskryminacja, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji
lub wszelką inną znaczna szkodą gospodarczą lub społeczną,</td></tr>
<tr><td>2</td><td>Niewielkie</td><td>Niewielki wpływ na prawa lub wolności osób. Niewielkie praktyczne możliwości zaszkodzenia osobie</td></tr>
<tr><td>3</td><td>Istotne</td><td>Istotny wpływ na prawa lub wolności osób. Istnieją realne możliwości zaszkodzenia osobie ale wymagają dodatkowych działań lub połączenia z danymi z innych źródeł</td></tr>
<tr><td>4</td><td>Duże</td><td>Duży wpływ na prawa lub wolności osób. Istnieją bezpośrednie możliwości zaszkodzenia osobie. Osoba powinna podjąć działania zapobiegawcze aby się przed nimi ochronić.</td></tr>
</table>

5	Bardzo duże	Bardzo duży wpływ na prawa lub wolności osób. Szkoda dla osoby jest pewna lub niemal pewna i wymagać będzie natychmiastowych działań ze strony osoby, której dane dotyczą (np. zastrzeżenie dokumentu tożsamości)	2) jeżeli osoby, których dane dotyczą, mogą zostać zbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi, 3) jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa, 4) jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych, 5) jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci, jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą

*Należy ocenić równocześnie wszystkie rodzaje skutków. Podczas oceny należy brać pod uwagę **najbardziej prawdopodobny** do wystąpienia skutek. Jeżeli z ryzykiem nie wiąże się dany rodzaj skutku należy wybrać wartość jeden.

§ 8
[Ustalenie wartości ryzyka]

Bazowym wzorem opisującym wartość ryzyka jest formuła wykorzystująca wartości punktowe prawdopodobieństwa i skutków wystąpienia ryzyka:

WR = P_R x max{S_D, S_C, S_W, S_N, S_I, S_P, S_K}

Gdzie:
WR – Wartość ryzyka
P_R - prawdopodobieństwo wystąpienia ryzyka
S_D – Skutek dla realizacji działania
S_C – Skutek dla ciągłości działalności
S_W – Skutek wizerunkowy
S_N – Skutek naruszenia praw lub wolności osób fizycznych
S_I – Skutek w zakresie bezpieczeństwa informacji
S_P – Skutek naruszenia prawa i procedur

S_K – Skutek w zakresie korupcji

Wszelkie opisy przyporządkowane do poszczególnych wartości na przyjętych w metodyce skalach oceny mają charakter pomocniczy. Dla oceny ryzyka kluczowym jest wybór odpowiedniej wartości na skali, która dla danego ryzyka nie zawsze będzie korespondować z opisem pomocniczym.

§ 9
[Ewaluacja ryzyka]

1. **Celem ewaluacji ryzyka** jest porównanie uzyskanej wartości ryzyka z wcześniej założonymi kryteriami akceptowalności i wskazanie poziomu ryzyk oraz wskazanie ryzyk nieakceptowalnych na bazie wcześniej ustalonych kryteriów.
2. **Efektem ewaluacji ryzyka** jest stworzenie rankingu ryzyka (wskazanie ryzyk kluczowych – nieakceptowalnych) oraz porównanie ryzyk między sobą (priorytetyzacja ryzyka).
3. Wyznaczona podczas analizy wartość ryzyka podlega ewaluacji, czyli porównywana jest z określonym progiem akceptowalności ryzyka. W przypadku ryzyka nieakceptowalnego niezbędne jest przygotowanie planów postepowania z tym ryzykiem, zgodnie z **§ 10.**
4. W Zespole wyznaczono następujące poziomy ryzyka:

Poziom ryzyka	Kryteria akceptowalności
Ryzyka nieakceptowalne	**Są to ryzyka, których wartości kształtują się w przedziale od 15 do 25.** Wymagają natychmiastowego podjęcia działań minimalizujących ryzyko. Należy wypełnić formularz „Plan postępowania z ryzykiem nieakceptowalnym”.
Ryzyka istotne	**Są to ryzyka, których wartości kształtują się w przedziale od 5 do 14.** Wymagają wzmożonego monitorowania. Możliwe jest podjęcie decyzji o uruchomieniu działań minimalizujących ryzyko. Dopuszcza się wypełnienie formularza „Plan postępowania z ryzykiem nieakceptowalnym”, decyzję o wypełnieniu podejmuje Właściciel ryzyka.
Ryzyka akceptowalne	**Są to ryzyka, których wartości kształtują się w przedziale od 1 do 4.** Nie wymagają podejmowania działań minimalizujących ryzyko. Nie wymagają wypełnienia formularza „Plan postępowania z ryzykiem nieakceptowalnym”

Pomocnicza macierz ryzyka:

Skutki (pkt)						
Bardzo duże (5)	5	10	15	20	25	
Duże (4)	4	8	12	16	20	
Istotne (3)	3	6	9	12	15	
Niewielkie (2)	2	4	6	8	10	
Nieznaczące (1)	1	2	3	4	5	
	Znikome (1)	Mało prawdopodobne (2)	Prawdopodobne (3)	Bardzo prawdopodobne (4)	Prawie pewne (5)	Prawdopodobieństwo (pkt)

5. Po dokonaniu analizy ryzyk Właściciel ryzyka, Dyrektor lub osoba upoważniona może wskazać konieczność umieszczenia w rejestrze ryzyk kolejnych ryzyk dla danego działania lub aktywa.

§ 10

[Przygotowanie planów postępowania z ryzykiem]

1. **Celem przygotowania planów postepowania z ryzykiem** jest wskazanie sposobu postępowania z ryzykiem nieakceptowalnym, efektem czego jest plan postępowania z ryzykiem nieakceptowalnym.
2. W odniesieniu do każdego ryzyka nieakceptowalnego Właściciel ryzyka powinien wskazać rozwiązania (reakcje), jakie chce wprowadzić, aby ryzyko to zmniejszać w przyszłości.

3. Decyzje o wdrożeniu planu postępowania z ryzykiem w zależności od jego znaczenia w ramach danego rodzaju podejmuje:
   1) Właściciel ryzyka w porozumieniu z Dyrektorem,
   2) Dyrektor,
   3) Zespół ds. kontroli zarządczej
4. Dla ryzyk w obszarze ochrony danych osobowych, w przypadku gdy ryzyko naruszenia praw lub wolności osób jest na poziomie nieakceptowalnym należy dokonać oceny skutków przetwarzania, zgodnie z odrębną procedurą oceny skutków dla ochrony danych osobowych – zgodnie z Procedurą bezpieczeństwa ochrony danych osobowych w Zespole.
5. W celu określenia sposobu postępowania z ryzykiem należy przeanalizować**:**
   1) przyczyny ryzyka i możliwe scenariusze,
   2) skuteczność istniejących mechanizmów kontroli/zabezpieczeń, tj. zakres, w jakim przeciwdziałają ryzyku lub minimalizują jego skutki, ich skuteczność i efektywność,
   3) koszty i korzyści związane z wdrożeniem planu postępowania z ryzykiem nieakceptowalnym.
6. Przyjmuje się, że w odniesieniu do ryzyka nieakceptowalnego można podjąć następujące rodzaje postępowania:

Postępowanie	**Opis**
Unikanie ryzyka poprzez decyzję o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko	Świadoma decyzja o nieangażowaniu się lub odejściu od ryzyka, działanie w celu eliminacji narażenia na konkretne ryzyko, odejście od działań, które wiążą się z ryzykiem.
Podjęcie ryzyka lub zwiększenie ryzyka w celu wykorzystania szansy	Polega na podjęciu działań, które zwiększą możliwość wystąpienia ryzyka lub działań, które wiążą się z wysokim ryzykiem, a które doprowadzą do uzyskania większych korzyści.
Łagodzenie – zmiana prawdopodobieństwa lub skutków	Polega na podjęciu działań mających na celu minimalizację prawdopodobieństwa lub skutków wystąpienia ryzyka lub obu jednocześnie, np. poprzez eliminację przyczyn ryzyka.
Dzielenie ryzyka z inną stroną lub stronami	Ograniczenie prawdopodobieństwa i skutków wystąpienia danego zdarzenia poprzez przekazanie w całości lub częściowo innej stronie.
Tolerowanie ryzyka (akceptacja ryzyka)	Niepodejmowanie dodatkowych działań w odpowiedzi na ryzyko w sytuacji, gdy ryzyko jest zarządzane w sposób wystarczający, akceptacja potencjalnych korzyści lun ciężaru skutków, wynikających z konkretnego ryzyka, przyjmuje się, iż ryzyka skrajne, nieakceptowalne można zaakceptować w przypadku braku możliwości podjęcia działań ograniczających poziom danego ryzyka

7. Wdrożone plany postępowania z ryzykiem nieakceptowalnym docelowo mogą stać się zmodyfikowanymi lub nowymi mechanizmami kontroli/zabezpieczeniami.
8. W ramach planu postępowania z ryzykiem zalecane jest przedstawienie kilku propozycji alternatywnych rozwiązań minimalizujących ryzyko.
9. Za wdrożenie planów postepowania z ryzykiem i za monitorowanie poszczególnych ryzyk odpowiadają Właściciele ryzyk.

§ 11
[Monitorowanie, komunikacja i konsultacja ryzyka]

1. Monitorowanie ryzyka to proces obserwacji wdrożenia reakcji na ryzyko, ciągłej obserwacji i nadzorowania zidentyfikowanych ryzyk, identyfikacji nowych ryzyk oraz systematycznego oceniania skuteczności mechanizmów kontrolnych. Monitorowanie ryzyka dostarcza informacji niezbędnych do podejmowania decyzji, które mają na celu zapobieganie wystąpieniu niepożądanych zdarzeń.
2. Proces monitorowania, komunikacji oraz konsultacji ryzyka ma na celu zapewnienie aktualnej informacji na temat ryzyka oraz stanu wdrożenia planów postepowania z ryzykiem, czego efektem jest uzyskanie adekwatnych i terminowych informacji na temat ryzyka i planów postepowania z ryzykiem.
3. Monitorowanie w ramach procesu zarzadzania ryzykiem odbywa się w odniesieniu do:
   1) wdrażanych planów postepowania z ryzykiem,
   2) skuteczności i efektywności stosowanych mechanizmów kontroli/zabezpieczeń,
   3) materializacji ryzyk oraz incydentów,
   4) zmian kontekstu wewnętrznego i zewnętrznego oraz jego wpływu na kryteria oceny ryzyka.
4. Monitorowanie ryzyka w Zespole jest procesem ciągłym. W ramach monitoringu podejmuje się czynności polegające na sprawdzeniu, czy:
   1) status ryzyka nie uległ zmianie,
   2) poziom ryzyka nie uległ zmianie,
   3) zidentyfikowano nowe ryzyka.
5. Na poziomie planów postępowania z ryzykiem nieakceptowalnym monitorowanie polega na sprawdzeniu czy status wdrażanych sposobów postępowania z ryzykiem nieakceptowalnym uległ zmianie:
   1) przed wprowadzeniem planu – „nie rozpoczęto”,
   2) w trakcie monitorowania wdrażane plany postępowania z ryzykiem powinny otrzymać status „W trakcie realizacji”,
   3) w przypadku zakończenia wdrażania, należy zmienić jego status na „Zakończony”. W tym przypadku należy zweryfikować listę mechanizmów kontroli/zabezpieczeń i poziom ich skuteczności oraz w przypadku zaistnienia takiej potrzeby rozszerzyć ich listę o nowy mechanizm lub zabezpieczenie, stanowiący efekt wdrożenia planu postępowania z ryzykiem,

4) w przypadku zakończenia wdrażania w związku z rezygnacją z realizacji planu należy zmienić status na „Wycofany z realizacji'.

6. Informowanie o ryzyku ma na celu osiągnięcie porozumienia, co do sposobu zarządzania ryzykiem poprzez wielostronną wymianę informacji pomiędzy osobami bezpośrednio zaangażowanymi w jego zarządzanie oraz innymi uczestnikami procesu zarządzania ryzykiem w Zespole. Skuteczna komunikacja pomaga w podejmowaniu decyzji dotyczących ryzyka.
7. W przypadku zidentyfikowania ryzyka wykraczającego poza kompetencje kierownika komórki organizacyjnej lub odnoszącego się do działania realizowanego przez inną komórkę organizacyjną wiedza na temat tego ryzyka jest przekazywana w formie pisemnej do osoby, która może nim skutecznie zarządzać. Analogiczną zasadę stosuje się do Właścicieli ryzyk niebędących kierownikami komórek organizacyjnych.
8. Właściciele ryzyk monitorują ryzyko w komórkach organizacyjnych, którymi zarządzają.
9. Pracownicy powinni być informowani o ryzykach dotyczących realizowanych przez nich działań, w szczególności w sytuacji kiedy nie brali oni udziału w identyfikacji ryzyka.
10. Właściciel ryzyka niezwłocznie powiadamia Zespół ds. Kontroli Zarządczej w przypadku identyfikacji nowego ryzyka przekraczającego akceptowalny poziom ryzyka, zmiany istotności ryzyka powodującej przekroczenie akceptowalnego poziomu ryzyka bądź wystąpienia zdarzenia związanego z ryzykiem przekraczającym akceptowalny poziom ryzyka.

§ 12
[Zgłaszanie incydentów]

1. Zgłaszanie incydentów pozwala na zapewnienie aktualnej i adekwatnej informacji na temat wystąpienia incydentów oraz przypadków materializacji ryzyka, co w efekcie pozwala uzyskać adekwatne informacje na temat prawdopodobieństwa i potencjalnych skutków wystąpienia ryzyka.
2. Każdy pracownik może zgłosić Właścicielowi ryzyka przepadek potencjalnej materializacji zidentyfikowanego lub nowego ryzyka.
3. Każdy incydent podlega akceptacji odpowiedniego Właściciela ryzyka.
4. W przypadku wystąpienia incydentu niedotyczącego zidentyfikowanego ryzyka, Właściciel ryzyka ma obowiązek zgłoszenia propozycji nowego ryzyka do rejestru ryzyka.

§ 13
[Rejestr ryzyk]

1. Rejestr zarządzanych ryzyk prowadzi Właściciel ryzyka.
2. Rejestr ryzyk zawiera co najmniej następujące dane:
   1) działanie/aktywo, w którym wskazano ryzyko,
   2) nazwę ryzyka,
   3) przyczyny wystąpienia ryzyka (wewnętrzne i zewnętrzne),
   4) skutki wystąpienia ryzyka,
   5) rodzaj ryzyka,
   6) charakter ryzyka (zagrożenie, szansa),
   7) właściciela ryzyka,
   8) mechanizmy kontroli ryzyka (zabezpieczenia),
   9) wyniki analizy ryzyka (ocena prawdopodobieństwa i wagi skutków),
   10) wartość ryzyka,
   11) poziom ryzyka,
   12) status ryzyka (aktualne, archiwalne),
   13) plan postepowania z ryzykiem nieakceptowalnym,

§ 14
[Dokumentowanie zarządzania ryzykiem
– wyznaczenie celów i ryzyk, wewnętrzny i zewnętrzny rejestr ryzyk oraz ich monitorowanie]

1. W terminie do 25 października każdego roku, Właściciele ryzyk przekazują do Zespołu ds. Kontroli Zarządczej w formie dokumentacyjnej (pisemnej) i elektronicznej:
   1) cele komórki organizacyjnej wraz z zadaniami i miernikami ich realizacji na **Załączniku nr 1**;
   2) wewnętrzny rejestr ryzyk komórki organizacyjnej na **Załączniku nr 2**.
2. Ustalając cele na dany rok, właściciele ryzyka w pierwszej kolejności powinni określić cele realizowane w komórce organizacyjnej, będące celami priorytetowymi Województwa, a także ryzyko związane z ich realizacją.
3. W terminie do 30 października każdego roku Zespół ds. Kontroli Zarządczej wyznacza cele i zadania Zespołu na kolejny rok wraz z załączonym rejestrem ryzyk i przedkłada po akceptacji Dyrektora Zespołu do Urzędu Marszałkowskiego do Departamentu nadzorującego do 31 października **- Załącznik nr 5 i Załącznik nr 6**.

§ 15

1. Właściciele ryzyk zobowiązani są udokumentować przeprowadzoną w podległej komórce analizę ryzyka poprzez utworzenie wewnętrznego rejestru ryzyk dla wyznaczonych celów i zadań komórki organizacyjnej.
2. Wewnętrzne rejestry ryzyk zawierają wszystkie rodzaje zidentyfikowanego ryzyka do wyznaczonych celów i zadań oraz podlegają aktualizacji na przestrzeni roku w taki sposób, by odzwierciedlał dynamiczny charakter ryzyka oraz sposób zarządzania komórkami organizacyjnymi.
3. Właściciele ryzyk przekazują do Zespołu ds. Kontroli Zarządczej do 8. dnia każdego miesiąca po zakończeniu kwartału wewnętrzny rejestr ryzyk **- Załącznik nr 2**.
4. W razie nieścisłości bądź zastrzeżeń dotyczących rejestrów przekazanych przez właścicieli ryzyk, Zespół ds. Kontroli Zarządczej zwraca się do właściciela ryzyk w celu wyjaśnienia, uzupełnienia bądź korekty rejestru.
5. Zbiorczy rejestr ryzyk udostępniany jest do wglądu dla wszystkich pracowników u pracownika ds. kontroli wewnętrznej – **Załącznik nr 3**.

§ 16

6. Raporty z monitoringu celów i zadań sporządza się w systemie kwartalnym na **Załączniku nr 4**.
7. Raporty z monitoringu celów i zadań przekazywane są do Zespołu ds. Kontroli Zarządczej w terminie do 8. dnia każdego miesiąca po zakończeniu danego kwartału.
8. Zespół ds. Kontroli Zarządczej przedstawia Dyrektorowi Zespołu zbiorczy raport z monitoringu celów i zadań do 10. dnia każdego miesiąca po zakończeniu kwartału. Po uzyskaniu akceptacji Dyrektora ZPKWŚ zbiorczy raport z monitoringu celów i zadań przekazywany jest do Departamentu nadzorującego w Urzędzie Marszałkowskim.

§ 17
[Zakończenie procedury]

1. Realizację procedury powierza się Zespołowi ds. kontroli zarządczej, nad którą nadzór sprawuje Przewodniczący Zespołu ds. kontroli zarządczej.

Załącznik nr 1
do Procedury zarządzania
ryzykiem w Zespole

WYZNACZENIE CELÓW ……STAŁYCH / ROCZNYCH
DZIAŁU …… ZESPOŁU PARKÓW KRAJOBRAZOWYCH WOJEWÓDZTWA ŚLĄSKIEGO
NA ROK ……

Cel Województwa	Typ celu (stały/ roczny)	Nazwa celu operacyjnego *	Dział realizujący	Miernik		
				Nazwa miernika	Częstotliwość pomiaru	Wartość Docelowa (planowana)
-1-	-3-	-4-	-5-	-6-	-7-	-8-

1) "* Przy wyznaczaniu celu i monitoringu jego realizacji należy dokonać analizy/przeglądu ryzyka (rejestr ryzyk), które będzie na bieżąco zarządzane i monitorowane. Dokumentowanie oceny / przeglądu ryzyka powinno odbywać się z przyjętą częstotliwością, nie rzadziej niż raz na pół roku."

……
(data i podpis Kierownika Działu)

Załącznik nr 2
do Procedury zarządzania
ryzykiem w Zespole

Wewnętrzny rejestr ryzyk …….Działu ……Zespołu Parków Krajobrazowych Województwa Śląskiego na rok ……*) / po …….. kwartale …….. roku*)
Opracowanie/aktualizacja* w dniu: ……

WZÓR

Rodzaj ryzyka	Działanie/ aktywo	Nazwa ryzyka	Przyczyny ryzyka	Skutki ryzyka	Charakter ryzyka	Właściciel ryzyka	Mechanizmy kontroli/ zabezpieczenia	Poziom prawdopodobieństwa	Poziom skutków								Wartość ryzyka	Poziom ryzyka	Status ryzyka	Plan postepowania z ryzykiem nieakceptowalnym	Status planu postepowania z ryzykiem nieakceptowalnym
									Realizacja	Ciągłość	Wizerunek	Bezpieczeństwo	Naruszenie prawa	Korupcja	Naruszenie praw	Poziom skutków (MAX)					

Zatwierdzam:

*wybrać właściwe *Objaśnienia do tabeli zawierającej ryzyka (należy wybrać właściwą opcję):*

1) Rodzaj ryzyka – operacyjne / bezpieczeństwa informacji / przetwarzanie danych osobowych / korupcja,
2) Charakter ryzyka – zagrożenie / szansa,
3) Status ryzyka – aktualne / archiwalne
4) Status planu postepowania z ryzykiem nieakceptowalnym – nie dotyczy / nie rozpoczęto / w trakcie realizacji / zakończony / wycofany z realizacji

……
(data i podpis Kierownika Działu) – niepotrzebne skreślić

Załącznik nr 3
do Procedury zarządzania
ryzykiem w Zespole

Zbiorczy rejestr ryzyk Zespołu Parków Krajobrazowych Województwa Śląskiego po …….. kwartale …….. roku
Opracowanie/aktualizacja*) w dniu: ……..

WZÓR

Symbol komórki organizacyjnej	Rodzaj ryzyka	Działanie/ aktywo	Nazwa ryzyka	Przyczyny ryzyka	Skutki ryzyka	Charakter ryzyka	Właściciel ryzyka	Mechanizmy kontroli/ zabezpieczenia	Poziom prawdopodobieństwa	Poziom skutków								Wartość ryzyka	Poziom ryzyka	Status ryzyka	Plan postepowania z ryzykiem nieakceptowalnym	Status planu postepowania z ryzykiem nieakceptowalnym
										Realizacja	Ciągłość	Wizerunek	Bezpieczeństwo	Naruszenie prawa	Korupcja	Naruszenie praw	Poziom skutków (MAX)					

Zatwierdzam:

*wybrać właściwe

Objaśnienia do tabeli zawierającej ryzyka (należy wybrać właściwą opcję):

5) Rodzaj ryzyka – operacyjne / bezpieczeństwa informacji / przetwarzanie danych osobowych / korupcja,
6) Charakter ryzyka – zagrożenie / szansa,
7) Status ryzyka – aktualne / archiwalne
8) Status planu postepowania z ryzykiem nieakceptowalnym – nie dotyczy / nie rozpoczęto / w trakcie realizacji / zakończony / wycofany z realizacji

……

(data i podpis Kierownika Jednostki) *) – niepotrzebne skreślić

Załącznik nr 4
do Procedury zarządzania
ryzykiem w Zespole

RAPORT Z MONITORINGU CELÓW PRIORYTETOWYCH WOJEWÓDZTWA
DZIAŁU …….. *) / ZESPOŁU PARKÓW KRAJOBRAZOWYCH WOJEWÓDZTWA ŚLĄSKIEGO *)
PO ……. KWARTALE ……ROKU *)

Cel Województwa	Komorka realizująca Zadanie[3]	Zadania służące realizacji celu lub etapy realizacji celu	Realizacja zgodnie z planem [4]	Miernik			Opis realizacji zadania oraz zaistniałych ryzyk, zmiana lub opóźnienie [5]
				Nazwa miernika	Wartość planowana	Wartość osiągnięta	
-1-	-2-	-3-	-4-	-5-	-6-	-7-	-8-

1. Niepotrzebne skreślić.
2. Wskazać np.: zakres dat, roczny, półroczny, według stanu na dzień…..itp.
3. W przypadku celu realizowanego przez kilka komórek należy wskazać koordynująca komórkę organizacyjną odpowiedzialną za przekazywanie danych w zakresie monitoringu celu oraz komórki współpracujące. Raporty zatwierdzony przez kierownika koordynującej komórki organizacyjnej.
4. Zaznaczyć właściwe
5. Należy opisać stan realizacji zadań oraz ryzyk, które wystąpiły (zmaterializowały się), rodzaj podjętych działań wraz z uzasadnieniem zmian w rejestrze ryzyk, uwzględniając opóźnienia w realizacji celu lub podjęcia zadań innych niż planowane. Jeżeli ryzyko lub opóźnienia nie wystąpiły należy to również odnotować. Do niniejszego raportu należy załączyć aktualny rejestr ryzyk.

……
(data i podpis
Kierownika Jednostki / Kierownika Działu*)*) – niepotrzebne skreślić

Załącznik nr 5
do Procedury zarządzania
[illegible]y [illegible]iem w Zespole

WZÓR

CELE PRIORYTETOWE WOJEWÓDZTWA ŚLĄSKIEGO/ ~~CELE JAKOŚCIOWE/ CELE BEZPIECZEŃSTWA INFORMACJI~~ NA ROK ……

ZESPOŁ PARKÓW KRAJOBRAZOWYCH WOJEWÓDZTWA ŚLĄSKIEGO

Zatwierdzam:

Cel	Komórka organizacyjna/ jednostka realizująca [1)]	Powiązania z celami strategicznymi[2)]	Zadania służące realizacji celu lub etapy realizacji celu	Miernik	
				Nazwa miernika	Planowana wartość

……

(data i podpis Kierownika Jednostki)

1) Niepotrzebne skreślić

2) W przypadku celu realizowanego przez kilka komórek/jednostek organizacyjnych należy wskazać koordynującą komórkę organizacyjną odpowiedzialną za przekazywanie danych w zakresie monitoringu celu priorytetowego oraz komórki współpracujące.

3) Dotyczy tylko celów priorytetowych Województwa. Proszę wskazać cel/cele z aktualnej strategii rozwoju Województwa lub innego dokumentu o charakterze strategicznym, z którym powiązany jest cel priorytetowy Województwa na dany rok.

Załącznik nr 6

do Procedury zarządzania ryzykiem
w Zespole

Rejestr ryzyk Zespołu Parków Krajobrazowych Województwa Śląskiego w Katowicach z/s w Będzinie na rok ……..
Opracowanie/aktualizacja* w dniu: ……..

WZÓR

Rodzaj ryzyka	Działanie/ aktywo	Nazwa ryzyka	Przyczyny ryzyka	Skutki ryzyka	Charakter ryzyka	Właściciel ryzyka	Mechanizmy kontroli/ zabezpieczenia	Poziom prawdopodobień	Poziom skutków								Wartość ryzyka	Poziom ryzyka	Status ryzyka	Plan postepowania z ryzykiem nieakceptowalnym	Status planu postepowania z ryzykiem nieakceptowalnym
									Realizacja	Ciągłość	Wizerunek	Bezpieczeństwo	Naruszenie prawa	Korupcja	Naruszenie praw	Poziom skutków (MAX)					

Zatwierdzam:

*wybrać właściwe

……
(data i podpis Kierownika Jednostki)

Objaśnienia do tabeli zawierającej ryzyka (należy wybrać właściwą opcję):

1) Rodzaj ryzyka – operacyjne / bezpieczeństwa informacji / przetwarzanie danych osobowych / korupcja,
2) Charakter ryzyka – zagrożenie / szansa,
3) Status ryzyka – aktualne / archiwalne
4) Status planu postepowania z ryzykiem nieakceptowalnym – nie dotyczy / nie rozpoczęto / w trakcie realizacji / zakończony / wycofany z realizacji