Załącznik Nr 1 do Zasad
funkcjonowania oraz metod monitorowania i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach i jednostkach organizacyjnych powiatu.

Procedura zarządzania ryzykiem

§ 1

1. Niniejszy dokument określa zakres, zasady i sposób funkcjonowania systemu zarządzania ryzykiem w Starostwie Powiatowym w Kielcach oraz jednostkach organizacyjnych powiatu.
2. Celem systemu zarządzania ryzykiem jest zapewnienie mechanizmów służących osiągnięciu wyznaczonych celów, poprawie jakości i efektywności zarządzania, zapewnienie kierownictwu niższego i wyższego szczebla wczesnej informacji o możliwych szansach lub zagrożeniach dla realizacji celów i zadań, uzyskanie bezpieczeństwa informacji, w tym danych osobowych jak i informacji niejawnych oraz wyeliminowaniu zakłóceń w osiąganiu celów i realizacji zadań bieżących oraz inwestycyjnych.
3. Za określenie celów i zadań wraz z określeniem systemu ich monitorowania, identyfikację, analizę i reakcję na ryzyko, a także jego aktualizację w wydziałach odpowiedzialny jest dyrektor wydziału.
4. Za określenie celów i zadań wraz z ich monitorowaniem, identyfikację, analizę i reakcję na ryzyko, a także jego aktualizację w jednostkach organizacyjnych powiatu odpowiedzialny jest kierownik danej jednostki (I poziom kontroli zarządczej).
5. Zarządzanie ryzykiem na II poziomie kontroli zarządczej realizowane jest w szczególności poprzez monitorowanie wykonania planu finansowego, analizę wyników audytów i kontroli, weryfikację ryzyk oszacowanych dla celów, zadań i obszarów.
6. Proces zarządzania ryzykiem musi być pisemnie udokumentowany.

§ 2

Użyte w niniejszej procedurze pojęcia oznaczają:

1) cele strategiczne – należy przez to rozumieć cele zawarte w Strategii Rozwoju Powiatu, wynikające z przyjętej misji i wizji, w perspektywie czasowej dłuższej niż rok,
2) cele operacyjne – należy przez to rozumieć cele określone w co najmniej rocznej perspektywie na poziomie wydziału/samodzielnej komórki organizacyjnej Starostwa lub jednostki organizacyjnej powiatu, które służą realizacji konkretnego celu strategicznego,
3) cele szczegółowe – należy przez to rozumieć cele zawarte w Strategii Rozwoju Powiatu, które służą realizacji celów strategicznych,
4) zadanie – należy przez to rozumieć czynność lub zespół czynności, które należy wykonać, aby osiągnąć zaplanowane cele,
5) obszar – należy przez to rozumieć zakres działalności jednostki/wydziału obejmujący zadania, czynności i procesy realizowane przez jednostki/wydziały, które mogą wykraczać poza zdefiniowane cele strategiczne, operacyjne i szczegółowe. Dzięki temu, obszar stanowi uzupełnienie analizy ryzyka, pozwalając na uwzględnienie wszystkich aspektów funkcjonowania jednostki/wydziału.
6) ryzyko – należy przez to rozumieć możliwość/prawdopodobieństwo wystąpienia zdarzeń, które będą miały negatywny wpływ na realizację zadań i założonych celów,
7) ryzyko w bezpieczeństwie informacji – należy przez to rozumieć potencjalną sytuację, gdzie określone zdarzenie wykorzysta podatność (słabość) aktywów powodując szkodę w organizacji,
8) wpływ ryzyka - należy przez to rozumieć skutki dla realizowania zadań i osiągania celów spowodowane przez zdarzenie objęte ryzykiem,
9) prawdopodobieństwo wystąpienia ryzyka - należy przez to rozumieć częstotliwość występowania zdarzenia objętego ryzykiem,
10) istotność ryzyka - należy przez to rozumieć iloczyn wpływu ryzyka (skutek) i prawdopodobieństwa jego wystąpienia,
11) analiza ryzyka – należy przez to rozumieć proces mający na celu określenie poziomu ryzyka poprzez ocenę prawdopodobieństwa oraz skutku jego wystąpienia,

12) akceptowany poziom ryzyka (ryzyko akceptowalne) - należy przez to rozumieć ustalony poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku,
13) zarządzanie ryzykiem – należy przez to rozumieć skoordynowane działania w celu kierowania i sterowania organizacją z uwzględnieniem ryzyka,
14) mechanizmy kontroli - należy przez to rozumieć wszystkie działania i procedury podejmowane lub ustanawiane w celu zwiększenia prawdopodobieństwa realizacji zadań i osiągania celów, w tym zwłaszcza:
    a) dokumentację systemu zarządzania i systemu bezpieczeństwa informacji (w szczególności procedury, instrukcje, wytyczne),
    b) dokumentowanie poszczególnych zdarzeń,
    c) zatwierdzanie operacji,
    d) podział obowiązków,
    e) nadzór,
    f) rejestrowanie istotnych odstępstw od zasad zapisanych w procedurach, instrukcjach czy wytycznych,
    g) ograniczenie dostępu do zasobów materialnych, finansowych.
15) aktywa – należy przez to rozumieć wszystko, co ma wartość dla organizacji:
    a) aktywa informacyjne (zasoby) - informacje, w tym dane osobowe,
    b) aktywa informatyczne (zasoby): - sprzęt (np. laptop, serwer, komputer, drukarka, dysk wymienny CD ROM, inne nośniki: slajd, mikrofilm, fax) - oprogramowanie (np. aplikacje, oprogramowanie systemowe), sieć, personel, siedziba , struktura organizacyjna.
16) podatność – cecha zasobu powodująca, że zasób jest narażony na działanie jednego lub wielu zagrożeń (np. podatnością serwerowni jest drewniana podłoga, zagrożeniem w tym przykładzie – pożar).
17) poufność informacji – należy przez to rozumieć zapewnienie, że informacja nie jest udostępniana lub ujawniana nieuprawnionym osobom, podmiotom lub procesom (tylko upoważnieni pracownicy mają dostęp do informacji).
18) integralność informacji – należy przez to rozumieć zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
19) dostępność informacji – należy przez to rozumieć zapewnienie, że informacje są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot (osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne),
20) rozliczalność – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (możliwość zidentyfikowania użytkownika) odpowiedzialnego za informację, jej przetwarzanie,
21) plan minimalizacji ryzyka – rozwiązanie techniczne lub działania organizacyjne minimalizujące ryzyko,
22) właściciel ryzyka – osoba odpowiedzialna za zarządzanie ryzykiem, mająca kompetencje do podjęcia działań zaradczych w stosunku do obszaru, którym zarządza,
23) ASI – Administrator Systemów Informatycznych, osoba w jednostce odpowiadająca za informatyczne zabezpieczenie systemów przetwarzających dane osobowe; pracownik jednostki/wykonawca usług informatycznych posiadający odpowiednią wiedzę i umiejętności w zakresie informatyki.

§ 3

1. Zarządzanie ryzykiem odbywa się według zasad:
    1) integracji z procesem zarządzania,
    2) powiązania z celami i zadaniami Starostwa i jednostek organizacyjnych powiatu,
    3) przypisania odpowiedzialności,
    4) proporcjonalności działań przeciwdziałających ryzyku do jego istotności.

2. Proces zarządzania ryzykiem obejmuje:
    1) identyfikację ryzyk,
    2) analizę ryzyk,
    3) ustalenie akceptowalnego poziomu ryzyk,
    4) reakcję na ryzyka,
    5) monitorowanie ryzyk.

§ 4

1) Przyjęto, iż podstawą do budowania ryzyka jest lista celów. Podczas identyfikacji ryzyka należy przeanalizować:
    a) cele i zadania Starostwa oraz jednostek organizacyjnych powiatu z uwzględnieniem najważniejszych celów wskazanych do realizacji,

b) poszczególne procesy realizowane przez Starostwo Powiatowe w Kielcach określone w ramach Zintegrowanego Systemu Zarządzania,
c) zagrożenia związane z osiąganiem celów i realizowaniem zadań,
d) incydenty bezpieczeństwa, niezgodności, zalecenia poaudytowe i pokontrolne,
e) czynności przetwarzania danych osobowych.

2) Ryzyka mogą mieć swoje źródła wewnątrz jednostki, jak również w środowisku, w jakim powiat funkcjonuje. Wśród czynników mogących mieć wpływ na wystąpienie ryzyk wymienia się:
   a) czynniki zewnętrzne – zmieniające się oczekiwania lub potrzeby, zmiany przepisów prawa, zagrożenia naturalne, zmiany gospodarcze, naciski na jednostkę z zewnątrz, zmiany technologii,
   b) czynniki wewnętrzne – charakter wykonywanej działalności, kultura organizacji, dostępne środki finansowe, plany i strategie, komunikacja, systemy informatyczne, poziom technologiczny, liczba pracowników i ich kwalifikacje, odpowiedzialność i postawa kierownictwa, liczba, rodzaj i wielkość dokonywanych operacji finansowych, przetwarzanie informacji oraz kategorie przetwarzanych danych osobowych.
3) Przykłady ryzyk występujących w ramach poszczególnych obszarów przedstawia załącznik nr 5.

§ 5
Wyznaczanie celów

1. Dyrektorzy jednostek organizacyjnych powiatu wyznaczają najważniejsze cele operacyjne, do których przypisywane są zadania oraz sposoby pomiaru, a następnie w terminie do dnia 1 grudnia każdego roku przekazują - na formularzu stanowiącym załącznik nr 2 do Zasad - do wydziału nadzorującego działalność jednostki.
2. W przypadku bezpośredniej podległości jednostki pod Starostę, Wicestarostę lub Członków Zarządu dyrektorzy jednostek organizacyjnych powiatu po uzyskaniu akceptacji nadzorującego Członka Zarządu przekazują informacje o których mowa w ust. 1 bezpośrednio do Wydziału Organizacji i Zarządzania Kryzysowego.
3. Dyrektorzy wydziałów wyznaczają najważniejsze cele operacyjne, do których przypisywane są zadania oraz sposoby pomiaru, a następnie - do 10 grudnia każdego roku - przekazują łącznie ze zweryfikowanymi celami operacyjnymi nadzorowanych jednostek organizacyjnych powiatu (po uzyskaniu akceptacji nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika) do Wydziału Organizacyjnego, zgodnie z załącznikiem nr 2 do Zasad.
4. Przy określaniu celów operacyjnych i zadań należy brać pod uwagę: ustawę o samorządzie powiatowym cele i kierunki działań zawarte w Strategii Rozwoju Powiatu Kieleckiego do roku 2030, Statut Powiatu Kieleckiego, Regulamin Organizacyjny Starostwa Powiatowego oraz cele zawarte w planach oraz programach.
5. Wydziały Starostwa określając cele operacyjne powinny uwzględnić procesy realizowane przez wydział ujęte w ramach Zintegrowanego Systemu Zarządzania.
6. Najważniejsze cele operacyjne i zadania dla wydziałów oraz jednostek organizacyjnych powiatu zostają przedstawione do zatwierdzenia Staroście.
7. Informacja o zatwierdzonych przez Starostę celach operacyjnych i zadaniach jest przekazywana wydziałom oraz jednostkom organizacyjnym powiatu przez Wydział Organizacyjnego
8. W przypadku utworzenia nowej jednostki organizacyjnej, dyrektor jednostki zobowiązany jest do przedłożenia najważniejszych celów operacyjnych, przypisanych zadań oraz sposobów pomiaru, zgodnie z wytycznymi zawartymi w formularzu stanowiącym załącznik nr 2 do Zasad, do właściwego wydziału nadzorującego działalność jednostki w terminie miesiąca od dnia utworzenia jednostki.
9. Dyrektor wydziału nadzorującego działalność jednostki dokonuje weryfikacji celów i zadań jednostki i po uzyskaniu akceptacji nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika przekazuje zweryfikowane cele i zadania jednostki niezwłocznie w terminie nie dłuższym niż 7 dni do Wydziału Organizacyjnego.
10. W sytuacji, gdy nowo powstała jednostka podlega bezpośrednio pod Starostę, Wicestarostę lub Członków Zarządu, dyrektor jednostki organizacyjnej powiatu po uzyskaniu akceptacji nadzorującego Członka Zarządu zobowiązany jest przekazać wymagane informacje, o których mowa w §5 ust. 1, bezpośrednio do Wydziału Organizacyjnego.

§ 6

Identyfikacja aktywów

1. W ramach systemu bezpieczeństwa informacji i ochrony danych osobowych, a także informacji niejawnych dyrektorzy wydziałów Starostwa, oraz dyrektorzy jednostek organizacyjnych powiatu identyfikują aktywa organizacji ze szczególnym uwzględnieniem aktywów informacyjnych (dokumentów w tym zawierających dane osobowe) oraz informatycznych oddzielnie dla każdego wydziału Starostwa i jednostki organizacyjnej.
2. W celu uporządkowania klasyfikacji, zasoby które mają podobną wartość oraz podobne wymogi bezpieczeństwa można łączyć w grupy. Grupy informacji stanowią powiązane ze sobą w logiczny sposób informacje funkcjonujące w Starostwie/ jednostkach organizacyjnych powiatu. Określenie zawartości poszczególnych grup możliwe jest dzięki nazwie odnoszącej się do zgrupowanych w ten sposób informacji oraz przy pomocy podanych przykładowych dokumentów wchodzących w ich skład.

3. Zidentyfikowane zasoby informacyjne oraz informatyczne poddaje się analizie pod względem ich istotności w organizacji. Zidentyfikowane zasoby opisuje się w „Karcie klasyfikacji zasobów i aktywów informacyjnych" stanowiącej załącznik nr 3 do Zasad.

4. Określenie ich wartości dla działalności i dla istotności organizacji następuje poprzez przydzielenie im odpowiednich wartości w obszarach poufności [P], dostępności [D] i integralności [I].

   WG = P + I + D

   gdzie:
   WG – wartość grupy informacji
   P – wartość współczynnika poufności danej grupy informacji
   I – wartość współczynnika integralności danej grupy informacji
   D – wartość współczynnika dostępności danej grupy informacji

Skala (wartość grupy informacji)	Poufność [P] (właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom)	Integralność [I] (właściwość polegająca na tym, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany)	Dostępność [d] (właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany (upoważniony) podmiot)
1	Informacja przetwarzana w aktywie informatycznym bądź zawarta w aktywie informacyjnym jest ogólnie dostępna dla pracowników Starostwa/jednostki oraz klientów Starostwa/jednostki	Nieautoryzowana zmiana informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym nie wpłynie na funkcjonowanie Starostwa/jednostki i nie ma wpływu na klientów. Naruszenie integralności informacji jest łatwe do wykrycia i naprawienia, skutki wywołane nieprawidłowością są łatwe do przewidzenia i naprawienia.	Dostęp do informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym może być opóźniony od 3 do 5 dni.
2	Udostępnienie informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym osobom nieupoważnionym może spowodować niewielkie	Nieautoryzowana zmiana informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym spowoduje nieznaczne problemy w funkcjonowaniu Starostwa/jednostki i ma niewielki wpływ na klientów.	Dostęp do informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym może być opóźniony od 1 do 3 dni.

	konsekwencje dla Starostwa/jednostki lub klientów, bez konsekwencji prawnych i/lub finansowych.	Nie wiąże się z odpowiedzialnością prawną i/lub finansową. Naruszenie integralności informacji jest możliwe do wykrycia i naprawienia, skutki wywołane wadliwą informacją są możliwe do skorygowania, wymaga to jednak pewnego nakładu pracy i/lub wiąże się z poniesieniem niewielkich nakładów finansowych	
3	Udostępnienie informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym osobom nieupoważnionym spowoduje konsekwencje dla Starostwa/jednostki lub klientów Starostwa, włącznie z prawnymi i/lub finansowymi. Informacje objęte tajemnicą, wynikającą z innych aktów prawnych (np. ordynacji podatkowej, tajemnicy bankowej, tajemnicy przedsiębiorstwa i pozostałych), informacje wrażliwe.	Nieautoryzowana zmiana informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym spowoduje poważne problemy w funkcjonowaniu Starostwa/jednostki oraz ma duży wpływ na klientów. Pociąga za sobą konsekwencje prawne i/lub finansowe. Naruszenie integralności informacji jest trudne lub wręcz niemożliwe do naprawienia, skutki wywołane wadliwą informacją wiążą się z poważnymi sankcjami (np. odszkodowawczymi lub karnymi). Usunięcie lub skorygowanie skutków wiąże się z poniesieniem znaczących nakładów finansowych	Dostęp do informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym musi być zapewniony w sposób nieprzerwany, brak dostępu może w skrajnych okolicznościach skutkować sankcjami karnymi lub odszkodowawczymi.

Wartość [WG]	Poziom ochrony	Nazwa poziomu ochrony
1 – 6	I	Ogólnie dostępne
7 – 9	II	Chronione

§ 7

Zarzadzanie ryzykiem

1. Po otrzymaniu informacji o akceptacji przedstawionych celów operacyjnych i zadań dyrektorzy wydziałów oraz dyrektorzy jednostek organizacyjnych powiatu dokonują identyfikacji i analizy ryzyka.
2. Dyrektorzy wydziałów oraz dyrektorzy jednostek organizacyjnych powiatu identyfikują ryzyka w ramach podległych im obszarów.
3. Identyfikacja oraz aktualizacja ryzyka w ramach podległych obszarów, związana z realizowanymi celami, zadaniami i projektami powinna się odbywać na bieżąco jako element rutynowego działania pracowników, nie rzadziej jednak niż raz w roku. Podstawą skutecznej identyfikacji jak i aktualizacji ryzyka jest zrozumienie wykonywanej działalności (celów i realizowanych zadań oraz ich możliwego wpływu na jakość życia społeczności lokalnej). Identyfikacja ryzyka powinna odbywać się, w miarę możliwości, przy współudziale pracowników merytorycznych, odpowiedzialnych bezpośrednio za dane zadanie. Przeprowadzając identyfikację oraz aktualizację zagrożeń w danych obszarach związanych z realizacją celów i zadań należy wziąć pod uwagę wykorzystywane aktywa w ramach wskazanego celu i

zadań (personel, sprzęt, oprogramowanie, dokumentacja, dane osobowe…) w tym wartość przetwarzanej grupy informacji oraz podatności i zagrożenia dla wykorzystywanych aktywów, przykłady podatności i zagrożeń przedstawia załącznik nr 4 do Zasad. Identyfikacja ryzyka powinna odpowiedzieć między innymi na pytania; co złego (jakie zagrożenie) może się wydarzyć (wpłynąć na brak realizacji celu i zadań), wskazać zagrożenia związane z utratą poufności, integralności, rozliczalności i dostępności do informacji, sprzętu i danych, w tym danych osobowych.

4. Dyrektorzy jednostek organizacyjnych powiatu w terminie do dnia 10 stycznia każdego roku, przekazują do wydziału nadzorującego w Starostwie wyniki analizy ryzyka wraz z planem minimalizacji ryzyka (w przypadku zidentyfikowania ryzyka o nieakceptowalnym poziomie) – zgodnie z załącznikiem nr 6 do Zasad.
5. W przypadku bezpośredniej podległości jednostki pod Starostę, Wicestarostę lub Członków Zarządu dyrektorzy jednostek organizacyjnych powiatu po uzyskaniu akceptacji nadzorującego Członka Zarządu przekazują informacje o których mowa w ust. 3 bezpośrednio do Wydziału Organizacyjnego.
6. W przypadku utworzenia nowej jednostki dyrektor jednostki zobowiązany jest przekazać do wydziału nadzorującego w Starostwie wyniki analizy ryzyka wraz z planem minimalizacji ryzyka (w przypadku zidentyfikowania ryzyka o nieakceptowalnym poziomie) – zgodnie z załącznikiem nr 6 do Zasad w terminie miesiąca od dnia zatwierdzenia celów nowo powstałej jednostki przez Starostę.
7. Dyrektor wydziału nadzorującego działalność jednostki zobowiązany jest przekazać zaakceptowane przez nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika wyniki analizy ryzyka jednostki wraz z planem minimalizacji ryzyka (w przypadku zidentyfikowania ryzyka o nieakceptowalnym poziomie) niezwłocznie w terminie nie dłuższym niż 7 dni do Wydziału Organizacyjnego.
8. W przypadku bezpośredniej podległości jednostki pod Starostę, Wicestarostę lub Członków Zarządu dyrektor jednostki organizacyjnej powiatu po uzyskaniu akceptacji nadzorującego Członka Zarządu przekazuje informacje o których mowa w ust. 6 bezpośrednio do Wydziału Organizacyjnego.
9. Dyrektorzy wydziałów, w terminie do 20 stycznia każdego roku, przekazują do Wydziału Organizacyjnego zaakceptowane przez nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika wyniki przeprowadzonej identyfikacji i analizy ryzyka celów własnych komórek organizacyjnych, a także nadzorowanych jednostek organizacyjnych powiatu wraz z planem minimalizacji ryzyka (w przypadku zidentyfikowania ryzyka
o nieakceptowalnym poziomie) - zgodnie z załącznikiem nr 6 do Zasad.
10. Analiza (ocena) zidentyfikowanych ryzyk polega na określeniu wpływu
i prawdopodobieństwa wystąpienia ryzyka, a następnie ustaleniu jego istotności.
11. Dyrektorzy jednostek organizacyjnych powiatu oraz dyrektorzy wydziałów zobligowani są do monitorowania podjętych działań wynikających z planu minimalizacji ryzyka - zgodnie z załącznikiem nr 7 do Zasad.
12. Ustalone metody ograniczania ryzyka do akceptowanego poziomu są również na bieżąco oceniane (monitorowane) wspólnie przez Inspektora Ochrony Danych w zakresie bezpieczeństwa informacji, danych osobowych oraz przez Administratora Systemów Informatycznych w zakresie bezpieczeństwa informatycznego, w ramach audytów ochrony danych osobowych i bezpieczeństwa informacji.
13. Na podstawie kompletnych informacji, o których mowa w ust. 4-6, Wydział Organizacyjny przygotowuje zbiorczy plan minimalizacji ryzyka i przedstawia do akceptacji Sekretarzowi,
a następnie do zatwierdzenia Staroście.
14. Kopia zbiorczego planu minimalizacji ryzyka przekazywana jest audytorowi wewnętrznemu.
15. Zarządzanie ryzykiem odnosi się również do zadań realizowanych na bieżąco.
16. W przypadku zmiany w poziomie zidentyfikowanych ryzyk lub wystąpienia nowego ryzyka dyrektorzy wydziałów i dyrektorzy jednostek organizacyjnych powiatu, zobowiązani są niezwłocznie przeprowadzić ponowną analizę ryzyka - zgodnie z załącznikiem nr 6 do Zasad.
17. O wystąpieniu nowego ryzyka, zmianie poziomu zidentyfikowanych ryzyk (wynikach ponownej analizy ryzyka) dyrektorzy wydziałów/dyrektorzy jednostek organizacyjnych powiatu są zobowiązani poinformować Wydział Organizacyjny w terminie do 7 dni od wystąpienia lub zmiany poziomu ryzyka. Informację należy przekazać zgodnie z załącznikiem nr 6 do Zasad wskazując zaistniałą zmianę.
18. W przypadku zmaterializowania się ryzyka, zagrażającego realizacji celów i zadań, informacja o tym jest przekazywana niezwłocznie do Wydziału Organizacyjnego, nie później jednak niż w terminie 7 dni od zmaterializowania się ryzyka.
19. Ryzyko podlega powtórnej ocenie w sytuacji zmiany celów i zadań.

§ 8
Metodologia oceny ryzyka

1. Ocena ryzyka rozpatruje trzy obszary:
   1) prawdopodobieństwo wystąpienia zagrożenia w ramach podległych obszarów, zagrożenie braku realizacji celów i zadań,
   2) podatność wykorzystywanych aktywów na zagrożenia,
   3) skutków potencjalnych zagrożeń,

   biorąc pod uwagę następstwa naruszenia lub utraty:
   a) poufności,
   b) integralności,
   c) dostępności,
   d) rozliczalności.

2. Ocena ryzyka polega na określeniu wpływu (skutku) i prawdopodobieństwa wystąpienia ryzyka w celu ustalenia istotności ryzyka i odbywa się według zasady

   I = S x P

   gdzie:
   I – współczynnik istotności ryzyka
   S – wielkość skutku bądź wpływu, jaki będzie miało ewentualne wystąpienie danego zdarzenia
   P – prawdopodobieństwo wystąpienia ryzyka

3. Ocena wpływu (skutku) oraz prawdopodobieństwa wystąpienia ryzyka określane jest w skali punktowej od 1 do 5.
4. W przypadku jednostek organizacyjnych powiatu wszelkich ocen należy dokonywać w kontekście specyfiki danej jednostki.

5. Określając prawdopodobieństwo wystąpienia zagrożenia w ramach podległych obszarów i zagrożenie braku realizacji celów i zadań, należy przeanalizować grupę wykorzystywanych informacji/aktywów informacyjnych i informatycznych pod kątem wpływu typowych podatności i wynikających z nich zagrożeń. Przykład podatności i zagrożeń zawiera załącznik nr 4 do Zasad.

6. Określając wpływ (skutek) wystąpienia zagrożenia w ramach podległych obszarów i zagrożenie braku realizacji celów i zadań należy wziąć pod uwagę okoliczność utraty integralności, poufności i dostępności wykorzystywanych aktywów.

   Szablon punktowej oceny prawdopodobieństwa wystąpienia i oddziaływania ryzyka
   1) Prawdopodobieństwo wystąpienia ryzyka (skala od 1 do 5)

Prawdopodobieństwo wystąpienia ryzyka	Opis szczegółowy	Wartość punktowa
Bardzo rzadkie lub prawie niemożliwe	Zdarzenie może zaistnieć jedynie w wyjątkowych okolicznościach (od 1 do 20% szansy, że wystąpi), a najprawdopodobniej w ogóle nie zaistnieje, nie wystąpiło dotychczas.	1
Małe prawdopodobieństwo	Istnieje małe prawdopodobieństwo (od 21 do 40%) zaistnienia tego zdarzenia.	2
Średnie prawdopodobieństwo	Zaistnienie zdarzenia jest średnio możliwe (od 41 do 60%), może wystąpić okazjonalnie.	3
Duże prawdopodobieństwo	Zaistnienie zdarzenia jest bardzo prawdopodobne (od 61 do 80%).	4
Prawie pewne	Istnieją uzasadnione powody by sadzić, że zdarzenie objęte ryzykiem wystąpi na pewno, może wystąpić wielokrotnie w ciągu roku (od 81 do 100% szans).	5

2) Wpływ (skutek) wystąpienia ryzyka (skala od 1 do 5)

Wpływ (skutek) wystąpienia ryzyka	Opis szczegółowy	Wartość punktowa
Nieznaczny	Rozwiązanie problemu będzie wymagało nieznacznego nakładu czasu/zasobów, znikomy wpływ na realizację celów i zadań organizacji, brak skutków prawnych, brak lub nieznaczny skutek finansowy, brak wpływu na bezpieczeństwo pracowników, brak wpływu na wizerunek organizacji.	1
Mały	Rozwiązanie problemu będzie wymagało pewnego nakładu czasu/zasobów, mały wpływ na realizację celów i zadań, bez skutków prawnych, brak lub nieznaczny skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek organizacji, możliwe nieznaczne zakłócenia w działalności.	2
Średni	Rozwiązanie problemu będzie wymagało umiarkowanego nakładu czasu/zasobów, w tym kierownictwa wyższego szczebla, średni wpływ na realizację celów i zadań, umiarkowane konsekwencje prawne, mały lub średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek organizacji, możliwe umiarkowane zakłócenia w działalności.	3
Poważny	Rozwiązanie problemu będzie wymagało dużego nakładu czasu/zasobów, w tym kierownictwa wyższego szczebla, poważny wpływ na realizację zadania, w tym poważne zagrożenie terminu jego realizacji jak i osiągnięcie celu, poważne konsekwencje prawne, zagrożenie bezpieczeństwa pracowników, poważne straty finansowe, poważny wpływ na wizerunek organizacji, znaczące zakłócenia w działalności.	4
Katastrofalny	Rozwiązanie problemu będzie wymagało bardzo dużego nakładu czasu/zasobów, w tym kierownictwa wyższego szczebla, usunięcie skutków będzie bardzo trudne lub niemożliwe, brak realizacji zadania i brak realizacji celu, bardzo poważne i rozległe konsekwencje prawne, naruszenie bezpieczeństwa pracowników (negatywne konsekwencje dla ich życia i zdrowia), wysokie straty finansowe, utrata dobrego wizerunku organizacji w środowisku oraz w opinii publicznej, bardzo dotkliwe zakłócenia w działalności.	5

3) Mapa ryzyka

Prawdopodobieństwo → Skutek ↓	Bardzo rzadkie lub prawie niemożliwe	Małe prawdopodobieństwo	Średnie prawdopodobieństwo	Prawdopodobne	Prawie pewne
Katastrofalny	5	10	15	20	25
Poważny	4	8	12	16	20
Średni	3	6	9	12	15
Mały	2	4	6	8	10
Nieznaczny	1	2	3	4	5

Ryzyko nieznaczne	Ryzyko umiarkowane	Ryzyko poważne

7. Akceptowalny poziom ryzyka
   1) W Starostwie Powiatowym w Kielcach oraz we wszystkich jednostkach organizacyjnych powiatu *ryzykiem akceptowalnym jest ryzyko nieznaczne.*
   2) Ryzyko poważne i umiarkowane przekracza akceptowalny poziom ryzyka i wymaga ustalenia i podjęcia działań ograniczających to ryzyko.
   3) W przypadku ryzyk poważnych i umiarkowanych zaplanowane działania ograniczające ryzyko należy wdrożyć niezwłocznie w najkrótszym możliwym terminie przewidzianym na realizację działań.
8. Metodami przeciwdziałania ryzyku są:
   1) przeciwdziałanie ryzyku – podejmowanie działań pozwalających na likwidację ryzyka lub jego ograniczenie do akceptowalnego poziomu, np. poprzez wzmocnienie mechanizmów kontroli wewnętrznej (opracowanie pisemnych procedur, wytycznych, instrukcji) wbudowanych w realizowane procesy,
   2) przeniesienie ryzyka – poprzez przesunięcie określonych działań poza strukturę jednostki na podmioty zewnętrzne (wtedy odpowiedzialność przekazujemy w odpowiednich zapisach umowy) np. ubezpieczenie,
   3) przesunięcie w czasie (wycofanie się) – zawieszenie realizacji działań w całości lub części rodzących zbyt duże ryzyko gdy jest możliwe bez naruszenia ustawowego obowiązku realizacji procesu w określonym wymiarze,
   4) tolerowanie ryzyka – akceptowanie ryzyka, świadome przyjęcie na siebie skutków ryzyka np. w sytuacji gdy istnieją określone trudności w przeciwdziałaniu ryzyku lub gdy koszty przeciwdziałania ryzyku mogłyby przekroczyć przewidywane korzyści.

9. Monitorowanie i raportowanie

1) Monitorowanie ryzyka jest procesem ciągłym i obejmuje również ryzyka dot. realizacji bieżących zadań wynikających z Regulaminu Organizacyjnego. Oznacza to potrzebę reagowania na zmiany jakie na bieżąco zachodzą w czasie realizacji celów i zadań (m.in. zmiany przepisów, zagrożenia otoczenia zewnętrznego, dodatkowe zadania, realizacja projektów itp.).
2) W ramach monitorowania ryzyka dokonywany jest przegląd aktualnych ryzyk w celu uzyskania informacji, czy?
   a) ryzyko nadal występuje,
   b) pojawiło się nowe ryzyko,
   c) prawdopodobieństwo i wpływ ryzyka zmieniły się,
   d) stosowane mechanizmy ograniczające ryzyko są skuteczne i efektywne.

3) W odniesieniu do Starostwa oraz jednostek organizacyjnych powiatu obowiązuje system monitorowania i raportowania wg. następującego schematu:

Lp.	Poziom istotności ryzyka	Monitoring	Raportowanie na podstawie załącznika nr 7
1	Ryzyko nieznaczne	Monitoring ciągły, okresowa analiza	nie dotyczy
2	Ryzyko umiarkowane	Monitoring ciągły, cykliczna analiza	1 raz na pół roku
3	Ryzyko poważne	Monitoring ciągły, szczegółowa, bieżąca analiza	1 raz na kwartał

4) W przypadku ryzyka umiarkowanego należy przesłać do Wydziału Organizacyjnego informację dotyczącą monitorowania ryzyka (zgodnie z załącznikiem nr 7 do Zasad) raz na pół roku z zachowaniem następującej ścieżki:

1) dyrektorzy jednostek organizacyjnych powiatu raportują w terminie do 10 lipca danego roku (informacja półroczna) oraz do 10 stycznia roku następnego (informacja roczna) do wydziału nadzorującego w Starostwie.
2) w przypadku utworzenia nowej jednostki dyrektor jednostki przesyła pierwszą informację półroczną po zakończeniu półrocza w którym ryzyka zostały zatwierdzone przez Starostę, odpowiednio w terminach do 10 lipca danego roku (informacja półroczna) oraz do 10 stycznia roku następnego (informacja roczna) do wydziału nadzorującego w Starostwie.
3) w przypadku bezpośredniej podległości jednostki pod Starostę, Wicestarostę lub Członków Zarządu dyrektorzy jednostek organizacyjnych powiatu raportują zaakceptowane przez nadzorującego Członka Zarządu informacje półroczne i roczne bezpośrednio do Wydziału Organizacyjnego.
4) dyrektorzy wydziałów w imieniu swoim i podległej jednostki organizacyjnej, raportują zaakceptowane przez nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika w terminie do 20 lipca danego roku (informacja półroczna) oraz do 20 stycznia roku następnego (informacja roczna) do Wydziału Organizacyjnego.

5) W przypadku ryzyka poważnego należy przesłać do Wydziału Organizacyjnego informację dotyczącą monitorowania ryzyka (zgodnie z załącznikiem nr 7 do Zasad) raz na kwartał z zachowaniem następującej ścieżki:
   a) dyrektorzy jednostek raportują w terminach do 10 kwietnia, 10 lipca, 10 października danego roku oraz 10 stycznia roku następnego (informacje kwartalne) do wydziału nadzorującego w Starostwie,
   b) w przypadku utworzenia nowej jednostki dyrektor jednostki przesyła pierwszą informację kwartalną po zakończeniu kwartału w którym ryzyka zostały zatwierdzone przez Starostę odpowiednio w terminach do 10 kwietnia, 10 lipca, 10 października danego roku oraz 10 stycznia roku następnego (informacje kwartalne) do wydziału nadzorującego w Starostwie,
   c) w przypadku bezpośredniej podległości jednostki pod Starostę, Wicestarostę lub Członków Zarządu dyrektorzy jednostek organizacyjnych powiatu raportują zaakceptowane przez nadzorującego Członka Zarządu informacje kwartalne bezpośrednio do Wydziału Organizacyjnego.
   d) dyrektorzy wydziałów w imieniu swoim i podległej jednostki organizacyjnej, raportują zaakceptowane przez nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika w terminach do 20 kwietnia, 20 lipca, 20 października danego roku oraz do 20 stycznia roku następnego (informacje kwartalne) do Wydziału Organizacyjnego,
   e) Wydział Organizacyjny na podstawie informacji otrzymanych z wydziałów i jednostek organizacyjnych powiatu przygotowuje sprawozdania zbiorcze, które przedkłada do akceptacji Członkom Zarządu, Sekretarzowi, Skarbnikowi oraz do zatwierdzenia Staroście.
   e) kopie zatwierdzonych sprawozdań przekazywane są audytorowi wewnętrznemu.

§ 9

Monitorowanie realizacji celów i zadań

1. Należy stale monitorować realizację celów i zadań za pomocą określonych mierników.
11. Monitorowanie celów szczegółowych wynikających ze Strategii Rozwoju Powiatu odbywa się również w oparciu o zasady i przyjęty zestaw wskaźników określonych w Uchwale Nr 311/363/2022 Zarządu Powiatu w Kielcach z dnia 3 listopada 2022r. w sprawie zatwierdzenia „Wskaźników dla systemu monitorowania realizacji Strategii Rozwoju Powiatu Kieleckiego do roku 2030".
2. Zobowiązuje się dyrektorów wydziałów oraz dyrektorów jednostek organizacyjnych powiatu do przygotowania sprawozdań z realizacji najważniejszych celów i zadań wydziału oraz nadzorowanych jednostek organizacyjnych.
3. Dyrektorzy jednostek organizacyjnych powiatu, w terminie do dnia 7 lipca każdego roku, przekazują półroczne sprawozdanie z realizacji celów i zadań – zgodnie z załącznikiem nr 8 do Zasad oraz do dnia 15 stycznia roku następnego sprawozdanie roczne - zgodnie z załącznikiem nr 8 do Zasad.
4. W przypadku utworzenia nowej jednostki dyrektor jednostki przekazuje pierwsze półroczne sprawozdanie z realizacji celów i zadań po zakończeniu półrocza w którym najważniejsze cele operacyjne i zadania jednostki zostały zatwierdzone przez Starostę w terminie do dnia 7 lipca każdego roku, oraz do dnia 15 stycznia roku następnego sprawozdanie roczne - zgodnie z załącznikiem nr 8 do Zasad.

5. W przypadku bezpośredniej podległości jednostki pod Starostę, Wicestarostę lub Członków Zarządu dyrektorzy jednostek organizacyjnych powiatu raportują zaakceptowane przez nadzorującego Członka Zarządu sprawozdania półroczne i roczne bezpośrednio do Wydziału Organizacyjnego.
6. Dyrektorzy wydziałów, w terminie do 15 lipca każdego roku, przekazują zaakceptowane przez nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika do Wydziału Organizacyjnego półroczne sprawozdanie z realizacji celów własnych komórek organizacyjnych, a także nadzorowanych jednostek organizacyjnych - zgodnie z załącznikiem
   nr 8 do Zasad oraz w terminie do 20 stycznia roku następnego sprawozdanie roczne z realizacji celów i zadań własnych komórek organizacyjnych, a także nadzorowanych jednostek organizacyjnych - zgodnie z załącznikiem nr 8 do Zasad.
7. W przypadku, gdy istnieje zagrożenie dla osiągnięcia przyjętych celów lub zadania nie są prawidłowo realizowane, należy dołączyć do informacji stosowne wyjaśnienia oraz propozycje działań zapobiegawczych.
8. Wydział Organizacyjny na podstawie informacji otrzymanych z wydziałów i jednostek organizacyjnych powiatu przygotowuje sprawozdania zbiorcze, które przedkłada do akceptacji Członkom Zarządu, Sekretarzowi, Skarbnikowi oraz do zatwierdzenia Staroście.