Zarządzenie Nr 180 /2022
STAROSTY KIELECKIEGO
z dnia 14 listopada 2022 r.

w sprawie ustalenia zasad funkcjonowania, metod monitorowania i oceny systemu kontroli zarządczej w Starostwie Powiatowym w Kielcach i w jednostkach organizacyjnych Powiatu Kieleckiego.

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2022 r. poz. 1526) oraz art. 69 ust. 1 pkt 2 i 3 z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2022 r. poz. 1634 z późn. zm.) zarządzam, co następuje:

§ 1

Dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy wprowadza się obowiązek prowadzenia kontroli zarządczej w Starostwie Powiatowym w Kielcach i w jednostkach organizacyjnych Powiatu Kieleckiego zgodnie z zasadami określonymi w załączniku nr 1 do niniejszego Zarządzenia.

§ 2

Wykonanie Zarządzenia powierza się wszystkim pracownikom Starostwa Powiatowego w Kielcach oraz kierownikom jednostek organizacyjnych Powiatu Kieleckiego.

§ 3

Nadzór nad wykonaniem Zarządzenia sprawuje Sekretarz Powiatu.

§ 4

Traci moc Zarządzenie Nr 203/2021 Starosty Kieleckiego z dnia 9 listopada 2021 r. w sprawie ustalenia zasad funkcjonowania, metod monitorowania i oceny systemu kontroli zarządczej w Starostwie Powiatowym w Kielcach i w jednostkach organizacyjnych Powiatu Kieleckiego.

.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Mirosław Gębski

Załącznik Nr 1 do Zarządzenia Nr 180/2022
Starosty Kieleckiego
z 14 listopada 2022 r.

Zasady funkcjonowania oraz metody monitorowania i oceny systemu kontroli zarządczej w Starostwie Powiatowym w Kielcach i jednostkach organizacyjnych powiatu.

Rozdział 1
Podstawy prawne

§ 1

1. Niniejsze Zasady zostały opracowane na podstawie ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U.2022 r. poz. 1526), Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247), a także w oparciu o wytyczne: zawarte w Komunikacie Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Min. Fin. Nr 15, poz. 84), zawarte w Komunikacie Nr 3 Ministra Finansów z dnia 16 lutego 2011 r. w sprawie szczegółowych wytycznych w zakresie samooceny kontroli zarządczej dla jednostek sektora finansów publicznych (Dz. Urz. Min. Fin. Nr 2, poz. 11), zawarte w Komunikacie 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. poz. 56).

Rozdział 2
Objaśnienia

§ 2

Ilekroć w Zasadach jest mowa o:

1. Starostwie – należy przez to rozumieć Starostwo Powiatowe w Kielcach;
2. Radzie - należy przez to rozumieć Radę Powiatu Kieleckiego;
3. Zarządzie - należy przez to rozumieć Zarząd Powiatu w Kielcach;
4. Staroście - należy przez to rozumieć Starostę Kieleckiego;
5. Sekretarzu – należy przez to rozumieć Sekretarza Powiatu;
6. Skarbniku – należy przez to rozumieć Skarbnika Powiatu;
7. Głównym Księgowym – należy przez to rozumieć Głównego Księgowego Starostwa;
8. Dyrektorach wydziałów – należy przez to rozumieć dyrektorów wydziałów/kierowników samodzielnych komórek organizacyjnych/pracowników zajmujących samodzielne stanowiska pracy;
9. Dyrektorach jednostek – należy przez to rozumieć kierowników jednostek organizacyjnych powiatu;
10. Wydziale – należy przez to rozumieć wydziały/samodzielne komórki organizacyjne i samodzielne stanowiska;
11. Regulaminie Organizacyjnym – naleć przez to rozumieć Regulamin Organizacyjny Starostwa Powiatowego w Kielcach;

12. Kontrola - jest to czynność polegająca na sprawdzeniu stanu faktycznego i porównaniu ze stanem wymaganym (wyznaczonym) w normach prawnych, technicznych, ekonomicznych, regulaminach i instrukcjach sposobu postępowania (procedurach), oraz sformułowaniu wniosków i zaleceń pokontrolnych mających na celu zlikwidowanie nieprawidłowości, a także usprawnienie prac w Starostwie lub innej kontrolowanej jednostce;
13. ZSZ – Zintegrowany System Zarządzania w Starostwie Powiatowym w Kielcach obejmujący System Zarządzania Jakością wg PN-EN ISO 9001: 2015-10 oraz System Zarządzania Bezpieczeństwem Informacji wg PN-EN ISO/IEC 27001-06;
14. RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Rozdział 3
Zakres odpowiedzialności

§ 3

1. Kontrola zarządcza sprawowana jest na dwóch poziomach:
   1) I poziom - jednostki sektora finansów publicznych, w których zapewnienie kontroli zarządczej należy do obowiązków kierownika jednostki, tj. w przypadku: a) Starostwa - do Starosty, b) jednostek organizacyjnych powiatu - do dyrektorów tych jednostek;
   2) II poziom - Powiat, jako jednostka samorządu terytorialnego, w której zapewnienie kontroli zarządczej należy do przewodniczącego Zarządu Powiatu, tj. Starosty.
2. Kontrola zarządcza w Starostwie i jednostkach organizacyjnych powiatu funkcjonuje w oparciu o standardy kontroli zarządczej z uwzględnieniem specyfik ich działalności.
3. Dyrektorzy wydziałów, zgodnie z podziałem kompetencji wynikających z Regulaminu Organizacyjnego Starostwa Powiatowego w Kielcach, zobowiązani są do wykonywania kontroli zarządczej w ramach posiadanych uprawnień.
4. Dyrektorzy wydziałów Starostwa oraz dyrektorzy jednostek organizacyjnych powiatu ponoszą odpowiedzialność za działania podejmowane w celu kontroli i nadzoru procesów zachodzących w kierowanych przez siebie wydziałach/jednostkach organizacyjnych, w sposób dający Staroście zapewnienie, że:
   1) działania te są zgodne z obowiązującymi przepisami prawa, procedurami wewnętrznymi, standardami kontroli zarządczej oraz wytycznymi w zakresie samooceny kontroli zarządczej dla jednostek sektora finansów publicznych,
   2) cele operacyjne, służące realizacji celów strategicznych, są osiągane a zadania wykonywane prawidłowo i sprawnie,
   3) ryzyka związane z realizacją celów i zadań są na bieżąco identyfikowane, aktualizowane i monitorowane,
   4) zasady etycznego postępowania pracowników są przestrzegane i promowane,
   5) przepływ informacji jest efektywny i skuteczny,
   6) posiadane zasoby, w szczególności składniki majątku, dane osobowe i informacje niejawne są właściwie zabezpieczone i chronione, obowiązujące regulacje wewnętrzne są na bieżąco analizowane, aktualizowane i dostosowywane do zmieniających się potrzeb.

5. Do obowiązków osób wskazanych w ust. 3, jako nadzorujących wykonanie powierzonych im zadań, należy w szczególności:

1) organizacja pracy podległych pracowników w sposób zapewniający osiąganie celów strategicznych i operacyjnych,
2) zapewnienie prawidłowości, skuteczności i efektywności realizowanych działań,
3) bezpośredni nadzór nad poprawnym merytorycznie i sprawnym wypełnianiem obowiązków służbowych przez podległych pracowników,
4) sprawdzanie, czy wydatki realizowane są w sposób zgodny z prawem, celowy i oszczędny, z zachowaniem zasady uzyskiwania najlepszych efektów z danych nakładów w sposób umożliwiający terminową realizację zadań oraz w wysokości i terminach wynikających z wcześniej zaciągniętych zobowiązań,
5) bieżące monitorowanie zgodności realizacji celów i zadań z przyjętymi planami i założeniami,
6) zarządzanie ryzykiem zapewniające bieżącą identyfikację, analizę, monitorowanie oraz planowanie reakcji na zaistniałe ryzyka,
7) bieżąca analiza regulacji wewnętrznych i ich dostosowywanie do zmieniających się potrzeb.

6. Do realizacji zadań w zakresie systemu kontroli zarządczej w wydziałach Starostwa zobowiązani są wszyscy pracownicy a w jednostkach organizacyjnych powiatu dyrektorzy tych jednostek i podlegli im pracownicy na zasadach określonych przez tych dyrektorów.
7. Działania podejmowane w zakresie kontroli zarządczej powinny być:
   1) **adekwatne** – czyli odpowiednie do zadań realizowanych przez Starostwo/jednostkę organizacyjną powiatu i obejmujące cały zakres ich działalności,
   2) **skuteczne** – to znaczy faktycznie zabezpieczające Starostwo/jednostkę organizacyjną powiatu przed wystąpieniem lub skutkami danego ryzyka; oraz pozwalające na osiągnięcie zamierzonych celów,
   3) **efektywne** – to znaczy, że powinny powodować osiąganie przez Starostwo/jednostkę organizacyjną powiatu założonych celów oraz najlepszych, możliwych wyników działania przy wykorzystaniu najmniejszych możliwych nakładów.
8. System kontroli zarządczej podlega w sposób ciągły elastycznemu dostosowywaniu do zmieniających się potrzeb i uwarunkowań prawnych.
9. Utrzymania systemu kontroli zarządczej w Starostwie należy do wspólnych zadań wydziałów i zostało określone w Regulaminie Organizacyjnym.

Rozdział 4
Funkcjonowanie Kontroli Zarządczej w Starostwie Powiatowym w Kielcach

§ 4

1. Kontrola zarządcza w Starostwie i jednostkach organizacyjnych powiatu jest narzędziem zarządzania i stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań, w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Celem kontroli zarządczej jest zapewnienie w szczególności:
   1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi,
   2) skuteczności i efektywności działania,
   3) wiarygodności sprawozdań, w szczególności sprawozdań finansowych,
   4) ochrony zasobów – w tym w zakresie zabezpieczenia: składników majątku przed zniszczeniem, utratą i defraudacją oraz danych osobowych i informacji niejawnych,
   5) przestrzegania i promowania zasad etycznego postępowania przez wszystkich pracowników,
   6) efektywności i skuteczności przepływu informacji,

7) zarządzania ryzykiem tj. bieżącego identyfikowania i monitorowania ryzyk związanych z realizacją zadań i osiąganiem zamierzonych celów oraz podejmowania reakcji na ryzyka,
8) ciągłego doskonalenia procesów zarządzania.

2. **System kontroli zarządczej stanowi zintegrowany zbiór elementów obejmujących:**
   1) środowisko wewnętrzne,
   2) cele i zarządzanie ryzykiem,
   3) mechanizmy kontroli,
   4) informacja i komunikacja,
   5) monitorowanie i ocena.

Rozdział 5
Realizacja standardów Kontroli Zarządczej w Starostwie Powiatowym w Kielcach

§ 5
Środowisko wewnętrzne

W zakresie środowiska wewnętrznego obwiązują następujące zasady oraz rozwiązania:

1. Przestrzeganie wartości etycznych

1) Osoby zarządzające oraz pracownicy Starostwa są świadomi wartości etycznych przyjętych w jednostce. Znają i przestrzegają zasad określonych w Kodeksie etyki pracowników Starostwa Powiatowego w Kielcach.
2) Dyrektorzy wydziałów są odpowiedzialni za propagowanie wartości etycznych, które powinni respektować pracownicy. Wspierają i promują przestrzeganie wartości etycznych dając dobry przykład codziennym postępowaniem i podejmowanymi decyzjami. Identyfikują i na bieżąco niwelują przesłanki powodujące zachowania nieetyczne (sprzyjające podejmowaniu niewłaściwych działań) a następnie zapobiegają ich powstawaniu w przyszłości.
3) Pracownicy Starostwa prezentują wysoką kulturę osobistą i dbają o wysoki poziom zawodowej uczciwości, ściśle przestrzegają wszystkich obowiązujących przepisów prawa i procedur, są świadomi konsekwencji wynikających z nieetycznych zachowań lub działań niezgodnych z prawem. Każdy przypadek nieetycznego zachowania jest poddawany analizie i stanowi podstawę do oceny pracownika.
4) Pracownicy mają obowiązek dbania o dobro Starostwa jak i jego wizerunku, chronienia jego mienia oraz zachowania w tajemnicy i poufności informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, jak również przestrzegania innych tajemnic prawnie chronionych.
5) Pracownicy powinni organizować swoją pracę w sposób zapewniający prawidłowe, terminowe, rzetelne i właściwe pod względem formalno - prawnym i merytorycznym wykonywanie przydzielonych im zadań, a także w sposób zapewniający przetwarzanie danych osobowych i informacji niejawnych zgodnie z obowiązującymi przepisami prawa i procedurami.

2. Kompetencje zawodowe

1) Osoby zarządzające i pracownicy posiadają odpowiednie kwalifikacje, umiejętności, wiedzę oraz niezbędne doświadczenie.
2) Rekrutacja nowych pracowników do Starostwa przebiega w sposób zapewniający wybór najlepszego kandydata na dane stanowisko. Szczegółowe uregulowania dotyczące zasad naboru pracowników do Starostwa zawarte są w ustawie o pracownikach samorządowych oraz w zarządzeniu Starosty w sprawie wprowadzenia Regulaminu naboru na wolne stanowiska

urzędnicze w tym na kierownicze stanowiska urzędnicze w Starostwie Powiatowym w Kielcach.

3) Każdy nowo zatrudniony pracownik podejmujący po raz pierwszy pracę na stanowisku urzędniczym kierowany jest do odbycia służby przygotowawczej, która ma zapewnić przygotowanie pracownika do należytego wykonywania obowiązków służbowych.
4) Praca zatrudnionego w Starostwie pracownika podlega okresowej ocenie. Szczegółowe regulacje dotyczące okresowych ocen pracowniczych określa ustawa o pracownikach samorządowych oraz zarządzenie Starosty Kieleckiego w sprawie wprowadzenia regulaminu przeprowadzania okresowej ceny. Celem okresowych ocen jest m.in.: ułatwienie planowania rozwoju pracownika, podejmowania decyzji w zakresie przeszeregowań pracowników oraz usprawnienia funkcjonowania systemu motywacyjnego.
5) Starosta zapewnia rozwój kompetencji zawodowych pracowników Starostwa oraz osób zarządzających poprzez system szkoleń i samokształcenia zgodnie z zasadami określonymi w ustawie Kodeks pracy, ustawie o pracownikach samorządowych oraz w zarządzeniu Starosty Kieleckiego w sprawie wprowadzenia procedury podnoszenia kwalifikacji zawodowych pracowników Starostwa Powiatowego w Kielcach, a także w przepisach szczególnych.

3. Struktura organizacyjna

1) Strukturę organizacyjną Starostwa ustala Zarząd Powiatu w Regulaminie Organizacyjnym Starostwa.
2) Struktura jest okresowo przeglądana i dostosowywana do zmieniających się przepisów prawa i potrzeb Starostwa.
3) Dyrektorzy wydziałów w sposób ciągły analizują przepisy prawa i zobowiązani są do składania wniosków mających na celu aktualizację Regulaminu Organizacyjnego Starostwa.
4) Każdy pracownik posiada ustalony na piśmie zakres obowiązków, który podlega aktualizacji.

4. Delegowanie uprawnień

1) Zakres uprawnień powierzonych poszczególnym pracownikom Starostwa jest określony w pisemnych, imiennych upoważnieniach, stosownie do rangi podejmowanych decyzji i czynności (np. kontrolnych, gospodarowania mieniem) stopnia ich złożoności i związanego z nimi ryzyka.
2) Upoważnienia są rejestrowane i przechowywane w rejestrze upoważnień, w aktach osobowych pracowników oraz w wydziałach merytorycznych odpowiedzialnych za przygotowywanie stosownych upoważnień. Delegowanie uprawnień jest potwierdzane podpisem osoby upoważnionej.
3) Sposób rejestrowania i sprawowania nadzoru nad upoważnieniami i pełnomocnictwami w Starostwie Powiatowym w Kielcach, zasady tworzenia tych dokumentów, organizację obiegu i ich przechowywania określa zarządzenie Starosty Kieleckiego w sprawie zasad udzielania upoważnień i pełnomocnictw przez Starostę Kieleckiego oraz sposobu ich rejestrowania i sprawowania nadzoru nad upoważnieniami i pełnomocnictwami w Starostwie Powiatowym w Kielcach.

§ 6
Cele i zarządzanie ryzykiem

1. Misja Starostwa

Misja Starostwa zawarta jest w Polityce Zintegrowanego Systemu Zarządzania.

2. Określanie celów i zadań, monitorowanie i ocena ich realizacji

W ramach określania celów działalności i zarządzania ryzykiem podjęte działania i nałożone obowiązki w celu spełnienia wymagań standardów w tym obszarze, zostały zawarte w **załączniku nr 1** do niniejszych Zasad.

§ 7
Mechanizmy kontroli

1. Dokumentowanie systemu kontroli zarządczej

Elementem kontroli zarządczej w Starostwie jest system wprowadzonych mechanizmów kontroli, na który składają się regulaminy, zarządzenia, procedury wewnętrzne, w tym:

1) procedury związane z funkcjonowaniem Starostwa,
2) procedury o charakterze organizacyjno-prawnym,
3) procedury związane z zamówieniami publicznymi,
4) procedury finansowe,
5) procedury gospodarowania mieniem,
6) dokumenty określające zakres obowiązków, uprawnień i odpowiedzialności pracowników,
7) dokumenty kontroli i audytu wewnętrznego oraz inne dokumenty wewnętrzne, tj. instrukcje, wytyczne,
8) inne wewnętrzne dokumenty wprowadzone m.in. w związku z funkcjonowaniem w Starostwie Zintegrowanego Systemu Zarządzania wg normy PN-EN ISO 9001:2015-10, PN ISO/IEC 27001:2017-06.

2. Wszystkie regulacje wewnętrzne stanowiące dokumentację systemu kontroli zarządczej w Starostwie są ze sobą spójne i dostępne dla wszystkich osób, dla których są niezbędne. Za właściwe dokumentowanie systemu kontroli zarządczej w Starostwie, zgodnie z właściwością merytoryczną, odpowiadają dyrektorzy wydziałów.

3. Nadzór

Zakres nadzoru nad realizacją zadań wynika z Regulaminu Organizacyjnego Starostwa. W trybie zwierzchnictwa służbowego prowadzony jest ciągły nadzór, którego celem jest zapewnienie osiągania przez Starostwo wyznaczonych celów i właściwe realizowanie zadań. Na system kontroli składają się:

1) **samokontrola**

a) do samokontroli zobowiązani są wszyscy pracownicy zatrudnieni w Starostwie Powiatowym bez względu na zajmowane stanowisko i rodzaj wykonywanej pracy. Samokontrola polega na kontroli prawidłowości wykonywania własnej pracy przez pracownika w oparciu o obowiązujące przepisy prawa i obowiązki wynikające z posiadanego zakresu czynności służbowych. Samokontrola realizowana jest w toku codziennego wykonywania zadań, w ramach powierzonych obowiązków służbowych,

b) w przypadku stwierdzenia nieprawidłowości pracownik zobowiązany jest podjąć niezbędne działania zgodnie ze sposobem postępowania uregulowanym w Procedurze ZSZ- 05 Działania korekcyjne, korygujące, zapobiegawcze.

2) **kontrola funkcjonalna**
kontrola funkcjonalna sprawowana jest przez Starostę, Wicestarostę, Członków Zarządu Powiatu, Sekretarza, Skarbnika i osoby znajdujące się na stanowiskach kierowniczych oraz urzędników wyznaczonych do realizacji powierzonych zadań. Obejmuje systematyczną ocenę stanu i efektów pracy osób nadzorowanych. Za kontrolę funkcjonalną w wydziałach odpowiadają dyrektorzy wydziałów.

3) **kontrola instytucjonalna**
Kontrola instytucjonalna realizowana jest przez:

a) audytora wewnętrznego, na podstawie rocznego planu zatwierdzonego przez Starostę,
b) pracowników Starostwa powołanych do przeprowadzenia kontroli wewnętrznych i zewnętrznych określonych w rocznych planach kontroli,
c) doraźne zespoły kontrolne powołane przez Starostę,
d) podmioty zewnętrzne, a w szczególności przez Regionalną Izbę Obrachunkową, Wojewodę Świętokrzyskiego, Najwyższą Izbę Kontroli oraz inne organy i instytucje uprawnione do sprawowania kontroli i nadzoru w zakresie działalności Starostwa.

4. Ciągłość działalności

1) W Starostwie zapewniona jest ciągłość funkcjonowania poprzez właściwy podział zadań, ustalenie zakresów czynności, upoważnień i zastępstw.
2) Na ciągłość funkcjonowania wpływa wprowadzony obowiązek ustalania planu urlopów.
3) Na wypadek przerw i awarii w działaniu systemów informatycznych w Starostwie zorganizowano system kopii zapasowych zgodnie z „IT-02 Procedurą tworzenia kopii zapasowych" oraz „IT-03 Procedurą testowania kopii zapasowych".
4) Celem procedury „Zarządzanie ciągłością działania" jest natomiast zapewnienie ciągłości działań związanych ze spełnieniem wymogów prawa, przy uwzględnieniu istniejących zagrożeń. Przedmiotem tej procedury jest ustalenie zasad tworzenia, wykonywania i testowania planów awarii.

5. Ochrona zasobów

1) W Starostwie funkcjonują procedury dotyczące ochrony zasobów. Pracownicy mają świadomość konieczności dołożenia należytej staranności w zakresie ich wykorzystania i bezpieczeństwa, a także odpowiedzialności dotyczącej ochrony zasobów.
2) Starostwo posiada stosowne zabezpieczenia, aby dostęp do jego zasobów materialnych, finansowych, informatycznych i informacyjnych miały jedynie upoważnione osoby. Osoby te są odpowiedzialne za ochronę i właściwe wykorzystywanie tych zasobów.
3) Pracownicy, którym powierzono odpowiedzialność za przekazany sprzęt, potwierdzają ten obowiązek podpisem w stosownej ewidencji.
4) Opracowano wewnętrzne procedury dotyczące ochrony informacji niejawnych, ochrony danych osobowych, wykorzystywania narzędzi informatycznych i obowiązków wynikających z ich stosowania przy realizacji zadań oraz przechowywania wytworzonej dokumentacji.
5) W przypadku danych informatycznych i informacyjnych istnieje odpowiedni system zabezpieczeń fizycznych i technicznych chroniący do nich dostępu.
6) Ochrona danych osobowych w systemie informatycznym, a także w formie fizycznej w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu odbywa się zgodnie z RODO.

6. Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych

W Starostwie funkcjonują następujące mechanizmy kontroli dotyczące operacji finansowych i gospodarczych:

1) przeprowadzanie wstępnej oceny celowości zaciągania zobowiązań finansowych i dokonywania wydatków,
2) rzetelne i pełne dokumentowanie, rejestrowanie operacji finansowych oraz gospodarczych. Wszystkie operacje finansowe i gospodarcze, a także inne znaczące zdarzenia są rzetelnie dokumentowane w celu umożliwienia prześledzenia każdej operacji finansowej, gospodarczej lub zdarzenia od samego początku, tj. w trakcie ich trwania i po zakończeniu,
3) zatwierdzanie (autoryzacja) operacji finansowych przez Starostę lub osoby przez niego upoważnione. Starosta lub upoważnieni przez niego pracownicy zatwierdzają wszelkie operacje finansowe i gospodarcze przed ich realizacją. Poszczególne czynności związane z realizacją operacji finansowych lub gospodarczych są wykonywane wyłącznie przez pracowników do tego upoważnionych,
4) podział kluczowych obowiązków. Kluczowe obowiązki dotyczące zatwierdzania, realizacji i księgowania operacji finansowych, gospodarczych i innych zdarzeń są rozdzielone pomiędzy różnych pracowników, z uwzględnieniem obowiązków i odpowiedzialności Skarbnika i Głównego Księgowego określonych w przepisach prawa.
5) weryfikacja operacji finansowych i gospodarczych przed i po realizacji.

7. Mechanizmy kontroli dotyczące systemów informatycznych

1) W Starostwie funkcjonują następujące mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych:

a) kontrola dostępu,
b) kontrola oprogramowania systemowego,
c) kontrola tworzenia i zmian w aplikacjach,
d) nadawanie uprawnień, ciągłość działalności i kontroli aplikacji.

2) Zarządzeniem Starosty ustalone zostały procedury wykonywania czynności kancelaryjnych z wykorzystaniem informatyki i oprogramowania oraz zarządzania oprogramowaniem. Niezależnie od nich funkcjonują dodatkowe procedury zabezpieczenia danych osobowych przetwarzanych w systemach informatycznych.

§ 8
Informacja i komunikacja

1. Bieżąca informacja

1) W celu skutecznej i prawidłowej realizacji zadań wszyscy pracownicy Starostwa mają zapewniony dostęp do informacji niezbędnych do realizacji powierzonych im zadań.
2) Wszyscy pracownicy Starostwa odpowiadają za to, aby udzielane przez nich informacje były aktualne, rzetelne i zrozumiałe a także przekazywane zgodnie z RODO.
3) Wszyscy pracownicy Starostwa odpowiadają za to, aby udzielana przez nich bieżąca informacja była aktualna, rzetelna, kompletna i zrozumiała, a także przetwarzana zgodnie z RODO, co umożliwia podejmowanie na jej podstawie właściwych działań i decyzji.
4) Dyrektorzy wydziałów zobowiązani są do wzajemnego uzgadniania swojej działalności oraz do współpracy przy wykonywaniu zadań w zakresie niezbędnym do zapewnienia koordynacji działania Starostwa, jako całości, w tym w szczególności zobowiązani są informować się wzajemnie o ustaleniach, zasadniczych rozstrzygnięciach i innych działaniach mających

związek z ich działalnością, których znajomość niezbędna jest dla zapewnienia koordynacji działania Starostwa, jako całości.

2. Komunikacja wewnętrzna i zewnętrzna

1) System komunikacji wewnętrznej umożliwia skuteczne przekazywanie potrzebnych informacji wewnątrz jednostki. Wiadomości przekazywane są w Starostwie poprzez pocztę elektroniczną, wewnętrzne komunikacyjne kanały informatyczne i na nośnikach papierowych.
2) W Starostwie funkcjonuje system elektronicznego obiegu dokumentów EZD PUW (system pomocniczy), który umożliwia śledzenie etapów realizacji spraw i zamieszczanie uwag i komentarzy w trakcie ich realizacji.
3) Odbywają się cykliczne spotkania Zarządu Powiatu z kadrą kierowniczą, podczas których następuje wymiana informacji pomiędzy kierownictwem a dyrektorami wydziałów oraz dokonywane są ustalenia, co do wspólnych działań wydziałów.
4) Dyrektorzy wydziałów odpowiedzialni są za skuteczny system wewnętrznej komunikacji w kierowanych przez siebie wydziałach, realizowany np. poprzez: cykliczne spotkania, narady, komunikaty mailowe, itp. Wymiana informacji następuje także za pośrednictwem wewnętrznego systemu obiegu dokumentów.
5) Cele i zadania na dany rok komunikuje się pracownikom w następujący sposób:
   a) poprzez umieszczenie na ogólnodostępnym serwerze w formie pliku komputerowego;
   b) ustnie w trakcie narad i spotkań,
   c) poprzez przekazanie zatwierdzonego dokumentu pracownikom komórek organizacyjnych zobowiązanych do współdziałania przy osiągnięciu danego celu.
6) Do obowiązków wszystkich pracowników należy przekazywanie niezbędnych informacji innym pracownikom mającym wpływ na osiągnięcie wyznaczonych celów i realizację zaplanowanych zadań.
7) W Starostwie funkcjonują mechanizmy zapewniające efektywny system wymiany informacji z podmiotami zewnętrznymi. Całość procesu jest dokumentowana, rejestrowana i przechowywana zgodnie z zasadami zawartymi w instrukcji kancelaryjnej oraz zachowaniem zasad Polityki Bezpieczeństwa Informacji Starostwa.

   W ramach komunikacji zewnętrznej:
   a) wyspecjalizowani pracownicy udzielają rzetelnych informacji np. w zakresie współpracy z mediami,
   b) w Starostwie zostały opracowane karty usług zawierające informacje odnośnie realizowanych zadań, które są na bieżąco aktualizowane zgodnie z Procedurą „Aktualizacja katalogu usług",
   c) informacje - oprócz tradycyjnych sposobów powiadamiania - przekazywane są również poprzez stronę internetową, przyjmowanie klientów w Starostwie, spotkania bezpośrednie, komunikaty i konferencje prasowe, materiały promocyjne.
8) Szczegółowe zasady udzielania informacji zostały opisane w Procedurze „Komunikacja z klientem „ oraz w Procedurze „Dostęp do informacji publicznej".

§ 9
Monitorowanie i ocena

1. Monitorowanie systemu kontroli zarządczej.

1) Dyrektorzy wydziałów zobowiązani są do ciągłego monitorowania i oceny poszczególnych elementów systemu kontroli zarządczej w celu bieżącego identyfikowania problemów i ich rozwiązywania
2) Dyrektorzy wydziałów są odpowiedzialni za ciągłe monitorowanie wartości poszczególnych ryzyk dotyczących zarządzanych przez nich obszarów oraz dostarczania Staroście na czas kompletnej i wiarygodnej informacji na temat ryzyk (zmianach poziomu ryzyk, nowych, dotychczas niezidentyfikowanych ryzykach).
3) Pracownicy Starostwa mają możliwość zgłaszania uwag dotyczących funkcjonowania systemu kontroli zarządczej.

2. Samoocena

1) Do przeprowadzania samooceny zobowiązani są wszyscy pracownicy Starostwa.
2) Raz w roku dokonuje się samooceny systemu kontroli zarządczej, samoocena przeprowadzana jest za pomocą elektronicznych ankiet. W szczególnych przypadkach dopuszcza się stosowanie ankiet w wersji papierowej.
3) Termin przeprowadzenia oraz wzór ankiety ustala koordynator ds. kontroli zarządczej i przedstawia Staroście celem akceptacji.
4) Wszyscy pracownicy Starostwa, w tym osoby zarządzające, zobowiązani są do dokonania samooceny systemu kontroli zarządczej w Starostwie poprzez udzielenie odpowiedzi na pytania zawarte w ankietach (odrębna ankieta dla kadry zarządzającej oraz odrębna dla pracowników).
5) Wyniki analizy ankiet z samooceny są podstawą do złożenia Staroście sprawozdania z przeprowadzonej samooceny kontroli zarządczej.

3. Audyt Wewnętrzny

1) Audytor Wewnętrzny prowadzi obiektywną i niezależną ocenę systemu kontroli zarządczej. Ocena ta dotyczy w szczególności adekwatności, skuteczności i efektywności mechanizmów kontroli zarządczej w jednostce. Działalność Audytora Wewnętrznego stanowi istotne wsparcie dla Starosty w realizowaniu zadań z zakresu kontroli zarządczej i wydatnie pomaga w realizacji celów i zadań Starostwa oraz jednostek organizacyjnych powiatu.
2) Do głównych zadań audytu wewnętrznego w ramach systemu zarządzania ryzykiem, należy:
    a) przeprowadzenie okresowej i niezależnej oceny jakości i efektywności procesu zarządzania ryzykiem oraz raportowanie wyników do Starosty,
    b) identyfikacja nowych ryzyk, jako wynik przeprowadzonych audytów wewnętrznych,
    c) przeprowadzenie oceny skuteczności środków kontroli ryzyka oraz planów minimalizacji ryzyka w trakcie prac audytowych.
3) Szczegółowe zasady prowadzenia audytu wewnętrznego oraz sposób i zakres oceny systemu kontroli zarządczej dokonywanej przez Audytora Wewnętrznego są uregulowane przepisami prawa i odrębnymi procedurami wewnętrznymi.

4. Uzyskanie zapewnienia o stanie kontroli zarządczej

1) Dyrektorzy wydziałów składają oświadczenie o stanie kontroli zarządczej według ustalonego wzoru określonego w zarządzeniu Starosty, za rok poprzedni do **15 lutego** roku następnego (**załącznik nr 9** do niniejszych Zasad).

2) Podstawą dla złożenia oświadczenia o stanie kontroli zarządczej w Starostwie za poprzedni rok kalendarzowy jest w szczególności:
   a) monitoring celów i zadań,
   b) samoocena kontroli zarządczej prowadzona zgodnie z ustaloną procedurą,
   c) monitoring zarządzania ryzykiem,
   d) prowadzony audyt wewnętrzny,
   e) wyniki przeprowadzonych kontroli wewnętrznych oraz kontroli zewnętrznych,
   f) wyniki przeprowadzonych auditów Zintegrowanego Systemu Zarządzania.

3) Analiza i ocena funkcjonowania kontroli zarządczej omawiana jest podczas przeglądu Zintegrowanego Systemu Zarządzania dokonywanego przez najwyższe kierownictwo przynajmniej raz do roku. Przegląd Zintegrowanego Systemu Zarządzania przeprowadzany jest zgodnie z Procedurą ZSZ-02 „Przegląd Zintegrowanego Systemu Zarządzania".

Rozdział 6
Ogólne wymagania systemu kontroli zarządczej w jednostkach organizacyjnych powiatu

§ 10

1. Dyrektorzy jednostek organizacyjnych powiatu zobowiązani są do:

1) wdrożenia adekwatnego, skutecznego i efektywnego systemu kontroli zarządczej, dostosowując go odpowiednio do zakresu zadań i wielkości zasobów kierowanej jednostki,
2) zapewnienia zgodności systemu kontroli zarządczej z treścią niniejszego zarządzenia, a także ze Standardami kontroli zarządczej dla sektora finansów publicznych zawartymi w Komunikacie nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. (Dz. Urz. MF Nr 15, poz. 84),
3) w przypadku stwierdzenia nieprawidłowości w działaniu kontroli zarządczej lub zidentyfikowaniu możliwości poprawy sposobu jej funkcjonowania dyrektorzy jednostek zobowiązani są do podejmowania działań naprawczych.

§ 11
Środowisko wewnętrzne

1. W zakresie środowiska wewnętrznego należy zapewnić:
   1) przestrzeganie wartości etycznych – zaleca się, aby wdrożone w jednostce procedury i wytyczne kontroli zarządczej zapewniały podnoszenie świadomości pracowników w zakresie przyjętych wartości etycznych oraz zapewniały ich przestrzeganie przy podejmowaniu decyzji i wykonywaniu powierzonych zadań. Należy zapoznać pracowników wszystkich szczebli organizacyjnych w jednostce z zasadami etycznego postępowania. Osoby zarządzające jednostką powinny wspierać i promować przestrzeganie wartości etycznych dając dobry przykład codziennym postępowaniem i podejmowanymi decyzjami,
   2) kompetencje zawodowe - zaleca się:
      a) przestrzeganie zasady, że pracownicy powinni posiadać wiedzę, umiejętności i doświadczenie, pozwalające skutecznie i efektywnie wypełniać powierzone zadania;
      b) wprowadzenie procedury rekrutacji zawierającej mechanizmy kontrolne konieczne do obiektywnego wyboru najlepszego kandydata na dane stanowisko,

c) wprowadzenie regulacji dotyczących wynagradzania, premiowania i nagradzania, dokonywania ocen pracowników, awansowania, rozwoju kompetencji zawodowych, szkoleń, które będą znane wszystkim pracownikom oraz jednakowo wobec nich stosowane.

3) struktura organizacyjna – należy dostosować strukturę organizacyjną do aktualnych celów i zadań jednostki. Zakres i rodzaj prowadzonych spraw oraz odpowiedzialności poszczególnych komórek organizacyjnych jednostki, a także aktualny zakres obowiązków, uprawnień i odpowiedzialności każdego pracownika należy określić w formie pisemnej w sposób przejrzysty i spójny. W celu realizacji powyższego wymagania zaleca się cykliczne dokonywanie przeglądów ustanowionego regulaminu organizacyjnego jednostki, wewnętrznych regulaminów organizacyjnych poszczególnych komórek organizacyjnych jednostki oraz opisów stanowisk pracy lub zakresów czynności pracowników jednostki.
4) delegowanie uprawnień – należy precyzyjnie określić zakres uprawnień delegowanych osobom kierującym komórkami organizacyjnymi jednostki lub pozostałym pracownikom, zakres delegowanych uprawnień musi być zgodny z prawem oraz odpowiedni do zakresu ponoszonej odpowiedzialności i ryzyka z nimi związanego. Powierzenie uprawnień lub obowiązków powinno być w formie pisemnej, w tym w formie pełnomocnictwa, upoważnienia. Przyjęcie uprawnień i obowiązków przez pracownika powinno być potwierdzone podpisem. Należy prowadzić zbiorczy rejestr wydanych pełnomocnictw i upoważnień.

§ 12
Cele i zarządzanie ryzykiem

1. Określenie misji jednostki sprzyja ustaleniu hierarchii celów i zadań oraz efektywnemu zarządzaniu ryzykiem. Należy rozważyć możliwość wskazania celu istnienia jednostki w postaci krótkiego i syntetycznego opisu misji.
2. W ramach określania celów działalności i zarządzania ryzykiem – podjęte działania i nałożone obowiązki w celu spełnienia wymagań standardów w tym obszarze zostały zawarte w **załączniku nr 1** do niniejszych Zasad.

§ 13
Mechanizmy kontroli

1. W zakresie mechanizmów kontroli należy zapewnić:
1) dokumentowanie systemu kontroli zarządczej – dokumentacja powinna być aktualna, spójna i dostępna dla wszystkich pracowników. Składają się na nią m.in.: procedury wewnętrzne, zarządzenia, uchwały, instrukcje, regulaminy, dokumenty określające zakresy obowiązków,
2) nadzór – należy prowadzić nadzór nad wykonywaniem zadań w celu ich oszczędnej, efektywnej i skutecznej realizacji,
3) ciągłość działania – należy zapewnić istnienie mechanizmów służących utrzymaniu ciągłości działalności jednostki. Przy czym zaleca się:
   a) sprawdzenie, czy funkcjonują w jednostce mechanizmy kontrolne zapobiegające zdarzeniom, które mogą spowodować zakłócenia jej działalności,
   b) wskazanie osób zastępujących poszczególne osoby kierujące komórkami organizacyjnymi jednostki podczas ich nieobecności oraz osób zastępujących każdego z pracowników w przypadku nieobecności,

c) zaprojektowanie i dopasowanie systemu kopii zapasowych, w sposób zapewniający spełnienie potrzeb jednostki z uwzględnieniem planu jego rozwoju, przewidywanego przyrostu danych i wykorzystywanych aplikacji,
d) określenie sposobu postępowania na wypadek wystąpienia nieoczekiwanych zakłóceń mających wpływ na funkcjonowanie komórek organizacyjnych jednostki, w szczególności przerw w działaniu systemów teleinformatycznych,

4) ochrona zasobów – należy zapewnić dostęp do zasobów jednostki jedynie dla osób upoważnionych oraz ustalić osobę odpowiedzialną za gospodarowanie zasobami, weryfikowanie, czy dostęp do poszczególnych zasobów, w tym w szczególności do danych osobowych jest limitowany oraz przypisany do właściwych osób, z zachowaniem zasad rozliczalności, integralności, poufności i minimalizacji danych, a także ograniczenia celu ich przetwarzania,
5) szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych – należy zapewnić poprzez:
a) rzetelne i pełne dokumentowanie i rejestrowanie operacji finansowych i gospodarczych,
b) zatwierdzanie operacji finansowych przez kierownika jednostki lub osoby przez niego upoważnione,
c) podział kluczowych obowiązków,
d) weryfikację operacji finansowych i gospodarczych przed i po ich realizacji.

6) mechanizmy kontroli dotyczące systemów informatycznych – należy określić mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych, obejmujące w szczególności mechanizmy zarządzania zmianami w infrastrukturze informatycznej oraz mechanizmy kontroli dostępu do zasobów informatycznych, mające na celu ich aktualizację oraz ochronę przed nieautoryzowanymi zmianami, odbieraniem, utratą lub ujawnieniem.

2. Zaleca się dokonanie przeglądu obowiązujących w jednostce procedur określających mechanizmy kontroli, w szczególności w zakresie zarządzania i dokumentowania operacji finansowych i udzielania zamówień publicznych, w celu weryfikacji, czy odpowiadają one zidentyfikowanym ryzykom.

§ 14
Informacja i komunikacja

1. W zakresie informacji i komunikacji ważne są:
1) bieżąca komunikacja – osobom zarządzającym i pracownikom należy zapewnić, w odpowiedniej formie i czasie, dostęp do rzetelnych informacji niezbędnych do wykonywania przez nich obowiązków,
2) komunikacja wewnętrzna i zewnętrzna – należy zapewnić efektywne mechanizmy przekazywania ważnych informacji w obrębie struktury jednostki organizacyjnej a także z podmiotami zewnętrznymi mającymi wpływ na osiągnięcie celów i realizację zadań.

§ 15
Monitorowanie i ocena

1. W zakresie monitorowania i oceny należy zapewnić:

1) monitorowanie systemu kontroli zarządczej – należy na bieżąco monitorować skuteczność poszczególnych elementów systemu kontroli zarządczej,
2) samoocena – należy, co najmniej raz w roku dokonać samooceny systemu kontroli zarządczej przez osoby zarządzające i pracowników jednostki. Samoocena powinna być odrębnym i udokumentowanym procesem. Szczegółowych wytycznych w zakresie samooceny kontroli zarządczej dla jednostek sektora finansów publicznych zawarte zostały w Komunikacie Nr 3 Ministra Finansów z dnia 16 lutego 2011 r.
3) audyt wewnętrzny – prowadzony w jednostce audyt wewnętrzny ma być działalnością obiektywną, której celem jest wspieranie kierownika jednostki w realizacji celów i zadań poprzez systematyczną ocenę kontroli zarządczej oraz czynności doradcze,
4) uzyskanie zapewnienia o stanie kontroli zarządczej – zobowiązuje się dyrektorów jednostek organizacyjnych do składania Staroście Kieleckiemu, w terminie do **15 lutego** każdego roku, oświadczeń o stanie kontroli zarządczej za rok poprzedni w kierowanej przez siebie jednostce. Wzór oświadczenia o stanie kontroli zarządczej stanowi **załącznik nr 9** do niniejszych Zasad. Źródłem uzyskania zapewnienia powinny być m.in. wyniki: monitorowania, samooceny oraz przeprowadzonych audytów i kontroli.

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 i zadań.
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 perspektywie rocznej 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) **ryzyko** – należy przez to rozumieć możliwość/prawdopodobieństwo wystąpienia zdarzeń, które będą miały negatywny wpływ na realizację zadań i założonych celów,
6) **ryzyko w bezpieczeństwie informacji** – należy przez to rozumieć potencjalną sytuację, gdzie określone zdarzenie wykorzysta podatność (słabość) aktywów powodując szkodę w organizacji,
7) **wpływie ryzyka** - należy przez to rozumieć skutki dla realizowania zadań i osiągania celów spowodowane przez zdarzenie objęte ryzykiem,
8) **prawdopodobieństwo wystąpienia ryzyka** - należy przez to rozumieć częstotliwość występowania zdarzenia objętego ryzykiem,

9) **istotności ryzyka** - należy przez to rozumieć iloczyn wpływu ryzyka (skutek) i prawdopodobieństwa jego wystąpienia,
10) **analiza ryzyka** – należy przez to rozumieć proces mający na celu określenie poziomu ryzyka poprzez ocenę prawdopodobieństwa oraz skutku jego wystąpienia,
11) **akceptowanym poziomie ryzyka** - należy przez to rozumieć ustalony poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku,
12) **zarządzanie ryzykiem** – należy przez to rozumieć skoordynowane działania w celu kierowania i sterowania organizacją z uwzględnieniem ryzyka,
13) **mechanizmach 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 (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.
14) **aktywach** – 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.
15) **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).
16) **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).
17) **integralność informacji** – należy przez to rozumieć zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
18) **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),
19) **rozliczalność** – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (możliwość zidentyfikowania użytkownika) odpowiedzialnego za informację, jej przetwarzanie,
20) **plan minimalizacji ryzyka** – rozwiązanie techniczne lub działania organizacyjne minimalizujące ryzyko,
21) **właściciel ryzyka** – osoba odpowiedzialna za zarządzanie ryzykiem, mająca kompetencje do podjęcia działań zaradczych w stosunku do obszaru, którym zarządza.

§ 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) 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.
2) Przykłady ryzyk występujących w ramach poszczególnych obszarów przedstawia **załącznik nr 5.**

§ 5

Wyznaczanie celów

1. Dyrektorzy jednostek organizacyjnych powiatu wyznaczają nie więcej niż 3 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 nie więcej niż 3 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 Organizacji i Zarządzania Kryzysowego, 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 Organizacji i Zarządzania Kryzysowego.

§ 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) 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 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 organizacji następuje poprzez przydzielenie im odpowiednich cen 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 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	Dostęp do informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym może być opóźniony od 3 do 5 dni.

		są łatwe do przewidzenia i naprawienia.	
2	Udostępnienie informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym osobom nieupoważnionym może spowodować niewielkie konsekwencje dla Starostwa/jednostki lub klientów, bez konsekwencji prawnych i/lub finansowych.	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. 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 wkładu pracy i/lub wiąże się z poniesieniem niewielkich nakładów finansowych	Dostęp do informacji lub danych osobowych przetwarzanych w aktywie informatycznym bądź zawartych w aktywie informacyjnym może być opóźniony od 1 do 3 dni.
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 celów operacyjnych i zadań dyrektorzy wydziałów oraz dyrektorzy jednostek organizacyjnych powiatu dokonują identyfikacji i analizy ryzyka.
2. Identyfikacja oraz aktualizacja ryzyka, związana z wyznaczonymi celami i realizowanymi zadaniami, 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 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 realizacji celów i zadań należy wziąć pod uwagę wykorzystywane aktywa w ramach realizowanego 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.
3. 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.
4. 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 Organizacji i Zarządzania Kryzysowego.
5. Dyrektorzy wydziałów, w terminie do **20 stycznia każdego roku**, przekazują do Wydziału Organizacji i Zarządzania Kryzysowego 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.
6. Analiza (ocena) zidentyfikowanych ryzyk polega na określeniu wpływu i prawdopodobieństwa wystąpienia ryzyka, a następnie ustaleniu jego istotności.
7. 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.
8. 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.
9. Na podstawie informacji, o których mowa w ust. 3, Wydział Organizacji i Zarządzania Kryzysowego przygotowuje zbiorczy plan minimalizacji ryzyka i w terminie do 31 stycznia przedstawia do akceptacji Sekretarzowi, a następnie do zatwierdzenia Staroście.
10. Kopia zbiorczego planu minimalizacji ryzyka przekazywana jest audytorowi wewnętrznemu.
11. Zarządzanie ryzykiem odnosi się również do zadań realizowanych na bieżąco.

12. 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.
13. O wystąpieniu nowego ryzyka, zmianie poziomu zidentyfikowanych ryzyk (wynikach ponownej analizy ryzyka) dyrektorzy wydziałów/dyrektorzy jednostek organizacyjnych powiatu są zobowiązani poinformować Wydział Organizacji i Zarządzania Kryzysowego w terminie **7 dni** od wystąpienia lub zmiany poziomu ryzyka.
14. W przypadku zmaterializowania się ryzyka, które może spowodować niezrealizowanie określonych celów, informacja o tym jest przekazywana niezwłocznie do Wydziału Organizacji i Zarządzania Kryzysowego.
15. Ryzyko podlega powtórnej ocenie w sytuacji zmiany celów i zadań.

§ 8
Metodologia oceny ryzyka

1. Ocena ryzyka rozpatruje trzy obszary:
   1) prawdopodobieństwo wystąpienia zagrożenia i braku realizacji celu,
   2) podatność wykorzystywanych aktywów na zagrożenia,
   3) skutków potencjalnych zagrożeń,

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

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

$$I = S \times P$$

   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 i braku realizacji celu 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 skutek wystąpienia zagrożenia i braku realizacji celu 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 (skutki) 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, 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, mały skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek organizacji, możliwe 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, średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek organizacji.	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.	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.	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.
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, 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 Organizacji i Zarządzania Kryzysowego 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 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 Organizacji i Zarządzania Kryzysowego.
    3) 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 Organizacji i Zarządzania Kryzysowego.
5) W przypadku ryzyka poważnego należy przesłać do Wydziału Organizacji i Zarządzania Kryzysowego 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 bezpośredniej podległości jednostki pod Starostę, Wicestarostę lub Członków Zarządu dyrektorzy jednostek organizacyjnych powiatu raportują zaakceptowane przez nadzorującego Członka Zarządu informacje kwartalne bezpośrednio do Wydziału Organizacji i Zarządzania Kryzysowego.
    c) 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 Organizacji i Zarządzania Kryzysowego,
    d) Wydział Organizacji i Zarządzania Kryzysowego 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.
8. 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 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 Organizacji i Zarządzania Kryzysowego.
5. Dyrektorzy wydziałów, w terminie do **15 lipca** każdego roku, przekazują zaakceptowane przez nadzorującego odpowiednio Członka Zarządu, Sekretarza, Skarbnika do Wydziału Organizacji i Zarządzania Kryzysowego 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.
6. 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.
7. Wydział Organizacji i Zarządzania Kryzysowego 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.

Załącznik Nr 2 do Zasad
funkcjonowania oraz metod monitorowania
i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach
i jednostkach organizacyjnych powiatu.

.....

Wydział/

jednostka organizacyjna

Arkusz najważniejszych celów Starostwa/ jednostki organizacyjnej powiatu

do realizacji w roku .....

Lp.	Cel strategiczny	Cel szczegółowy/operacyjny	Zadania służące realizacji celu	Termin realizacji celu/zadań	Mierniki określające stopień realizacji celu/zadań	Zakładana wartość miernika do osiągnięcia		Uwagi: Komórka organizacyjna/ osoba odpowiedzialna
						do 30 czerwca	do 31 grudnia	
1	2	3	4	5	6	7	8	9

.....

Data

.....

Podpis dyrektora

Akceptujący:

.....

Data

Załącznik Nr 3 do Zasad
funkcjonowania oraz metod monitorowania
i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach
i jednostkach organizacyjnych powiatu.

.....
Wydział/
jednostka organizacyjna

Karta klasyfikacji zasobów i aktywów informacyjnych

Grupa informacji-zasób	Ocena			WG-wartość Poziom ochrony
	Poufność	Integralność	Dostępność	

.....
(data)

.....
(podpis dyrektora)

Aktywa	Przykładowa podatność	Zagrożenie
Personel	Niewystarczająca obsada stanowisk. Utrata kluczowego pracownika.	Nieobecność pracownika – brak ciągłości działania
	Praca obcego personelu bez odpowiedniego nadzoru	Kradzież, kopiowanie lub inny nieuprawniony dostęp do informacji
	Niewystarczające przeszkolenie	Błędy związane z obsługą
	Niewłaściwe wykorzystanie sprzętu lub oprogramowania	Awaria sprzętu, trwała utrata danych.
	Brak zasad korzystania z urządzeń teleinformatycznych, brak procedur, brak kontroli.	Wykorzystanie urządzeń w sposób nieautoryzowany np.: przesyłanie wiadomości z danymi poufnymi przez e-mail z prywatnej strony WWW
	Brak komunikacji pomiędzy pracownikami i wydziałem	Niewłaściwe wykonywanie działań, opóźnienia w realizacji zadań
	Brak świadomości pracowników o wynikającym z tego zagrożeniu, brak szkoleń.	Plotkarstwo. Nieumyślne przekazywanie poufnych informacji.
Otoczenie fizyczne i infrastruktura	Niewłaściwa ochrona fizyczna budynku, pomieszczeń, drzwi i okien	Kradzież
	Niewłaściwa lub niedbała kontrola dostępu do budynku i pomieszczeń	Nieuprawniony dostęp osób trzecich np. celowe uszkodzenie.
	Lokalizacja budynku, niewłaściwy dobór pomieszczeń, brak klimatyzacji	Zawilgocenie
	Brak stałej konserwacji	Awaria systemu alarmowego. Awaria systemu kontroli dostępu.
	Brak procedur regulujących bezpieczeństwo aktywów	Utrata danych, Niezgodność z przepisami prawa, Nieautoryzowany dostęp
Sprzęt	Brak planu wymiany zużywających się części, zła obsługa, sprzęt niskiej jakości	Uszkodzenie urządzenia, wygaśnięcie wsparcia producenta.
	Niewłaściwa obsługa lub błędna instalacja urządzeń, błędnie napisana instrukcja, brak przeszkolenia pracowników. Użytkowanie sieci napięcia niezgodnie z przeznaczeniem.	Uszkodzenie urządzenia podczas obsługi
	Brak lub niewłaściwa kontrola zmian, błędnie napisana instrukcja, brak przeszkolenia pracowników	Błędy pracowników obsługujących klientów
	Brak stosownych procedur	Utrata nośnika z informacją, utrata laptopa
	Niezabezpieczone urządzenie do przechowywania danych	Kradzież danych lub dokumentów
	Brak procedur niszczenia nośników. Brak przestrzegania procedur.	Nieuprawniony dostęp do danych.
	Brak planów okresowej wymiany sprzętu.	Awaria urządzenia.
Teleinformatyka	Wilgotność, zalanie z rur C.O., podwyższenie temperatury, pożar (brak czujników temperatury, zalania i dymu), niezabezpieczone okno	Uszkodzenie lub unieruchomienie serwera
	Brak kopii zapasowych lub kopie zapasowe przechowywane w tym samym pomieszczeniu lub na tym samym serwerze	Oprogramowanie szkodliwe, siły wyższe, częściowe lub całkowite zniszczenie informacji
	Zmiana przeznaczenia lub likwidacja nośników pamięciowych bez trwałego usunięcia z nich poprzednich informacji wrażliwych	Nieautoryzowane przekazanie dostępu do informacji
	Przekazywanie haseł pracownikom, przesyłanie tekstem jawnym	Nieautoryzowany dostęp do informacji

	Brak stosowania polityki czystego pulpitu Komputera	Pobranie plików i informacji z pulpitu
Dokumentacja	Przechowywanie bez właściwej ochrony, Kopiowanie bez kontroli, Brak należytej uwagi ze strony użytkującego	Kradzież
	Pozostawione bez kontroli i nadzoru dokumenty w drukarkach lokalnych i sieciowych, faxach, kserokopiarkach; dokumenty wyrzucane do koszy na śmieci, brak niszczarek, bałagan na biurku,	Dostęp osoby niepowołanej do dokumentacji, zgubienie dokumentów.
	Bałagan na biurku, pozostawianie w biurach dokumentów niezabezpieczonych, przeznaczonych do archiwizacji.	Dostęp do dokumentów archiwalnych lub ich zniszczenie przez osoby nieuprawnione.
	Przestarzała instalacja elektryczna w pomieszczeniach biurowych	Pożar
	Przestarzała instalacji wodna i c.o. w pomieszczeniach	Zalanie archiwum
	Brak wylogowywania przy opuszczaniu stacji roboczej	Nieuprawniony dostęp do danych

Załącznik Nr 5 do Zasad
funkcjonowania oraz metod monitorowania
i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach
i jednostkach organizacyjnych powiatu.

Kategorie (obszary) ryzyka

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

Kategorie ryzyka	
Ryzyko finansowe	
Budżetowe	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów.
Strat majątkowych	Związane ze stratami finansowymi, które mogą być przedmiotem ubezpieczenia, np. ryzyko pożaru, wypadku.
Zamówień publicznych i zlecania zadań publicznych	Związane z podejmowaniem decyzji oraz udzielaniem zamówień publicznych lub zlecaniem zadań publicznych innym podmiotom, np. ryzyko naruszenia zasad, form lub trybu udzielania zamówień publicznych.
Odpowiedzialności finansowej	Związane z obowiązkiem zapłaty kwot pieniężnych tytułem np. odszkodowań, odsetek ustawowych, kar finansowych, kosztów procesowych.
Realizacja programów współfinansowanych ze środków Unii Europejskiej	Związane z wystąpieniem nieprawidłowości przy wykorzystaniu środków z Unii Europejskiej.
Ryzyko dotyczące zasobów ludzkich	
Personelu	Związane z liczebnością i kompetencjami pracowników, szkoleniami, wprowadzaniem nowych zadań bez zabezpieczenia kadrowego.
BHP	Związane ze zdrowiem pracowników i wypadkami przy pracy.
Ryzyko działalności	
Regulacji wewnętrznych	Związane z istnieniem i adekwatnością regulacji wewnętrznych.
Organizacji i podejmowania decyzji	Związane ze strukturą organizacyjną, organizacją pracy oraz przekazywaniem obowiązków i uprawnień, np. ryzyko nieprecyzyjnie określonych obowiązków, ryzyko braku formalnie powierzonych obowiązków, ryzyko nieodpowiedniej struktury organizacyjnej, ryzyko nieprawidłowo wydanej decyzji, zapewnienie terminowego ogłaszania aktów normatywnych, w tym przepisów prawa miejscowego.
Kontroli funkcjonalnej i samooceny	Związane z funkcjonowaniem systemu kontroli funkcjonalnej, np. ryzyko niedostatecznej kontroli, ryzyko nieskutecznych mechanizmów kontroli.

Ryzyko bezpieczeństwa informacji	
Niewłaściwej komunikacji	Związane z jakością informacji, na podstawie których podejmowane są decyzje, np. ryzyko braku komunikacji wewnętrznej i zewnętrznej.
Utraty informacji	Związane z kradzieżą urządzeń, nośników lub dokumentów, ujawnieniem danych, pobieraniem danych z niewiarygodnych źródeł, manipulowaniem urządzeniem oraz sfałszowaniem oprogramowania
Ryzyko awarii technicznej	Związane z awarią urządzenia, niewłaściwym funkcjonowaniem urządzeń, przeciążeniem systemu informacyjnego, niewłaściwym funkcjonowaniem oprogramowania, naruszeniem zdolności utrzymania systemu informacyjnego
Ryzyko nieautoryzowanego działania	Związane z nieautoryzowanym użyciem urządzeń, nieuprawnionym kopiowaniem oprogramowania, użyciem fałszywego lub skopiowanego oprogramowania, zniekształceniem danych, nielegalnym przetwarzaniem danych
Ryzyko utraty podstawowych usług	Związanego z utratą dostaw prądu, awarią systemu klimatyzacji (serwerownia), awarią urządzenia telekomunikacyjnego
Ryzyko zniszczenia fizycznego	Związane z pożarem, zalaniem, zniszczeniem urządzeń lub nośników
Ryzyko związane z wystąpieniem zjawiska naturalnego	Związane z wystąpieniem zjawisk pogodowych, sejsmicznych, klimatycznych oraz powodzi
Reputacji	Związane z reputacją Urzędu, np. ryzyko negatywnych opinii.
Systemów informatycznych	Związane z używanymi w Urzędzie systemami i programami informatycznymi oraz ochroną zawartych w nich danych, np. ryzyko awarii, ryzyko udostępnienia danych osobom nieuprawnionym, ryzyko nieuprawnionej modyfikacji danych.
Ryzyko zewnętrzne	
Gospodarcze	Związane z czynnikami ekonomicznymi, np. kursami walut, inflacją.
Środowiska prawnego	Związane ze skomplikowaniem i zmianami prawa oraz niejednolitym orzecznictwem.

Załącznik Nr 6 do Zasad
funkcjonowania oraz metod monitorowania i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach i jednostkach organizacyjnych powiatu.

.....

Wydział/

jednostka organizacyjna:

Arkusz ryzyk do najważniejszych celów Starostwa/ jednostki organizacyjnej powiatu na rok

Lp.	Cel strategiczny	Cel szczegółowy/ operacyjny	Zadania	WG Grupa wykorzystywanej informacji/aktywa informacyjne	Identyfikacja ryzyka	Analiza ryzyka			Plan minimalizacji ryzyka zaplanowane działania w celu obniżenia ryzyka (w przypadku ryzyk nieakceptowalnych)	Właściciel ryzyka
					Zdarzenie, które może zagrozić realizacji celów z uwzględnieniem zdarzeń dot. wykorzystywanych aktywów)	Prawdopodobieństwo wystąpienia danego zdarzenia P	Wpływ ryzyka (skutek) W	Istotność ryzyka I = PxW		
1	2	3	4	5	6	7	8	9	10	11

.....
Data

.....
Podpis dyrektora

Akceptujący:

.....
Data

Załącznik Nr 7 do Zasad
funkcjonowania oraz metod monitorowania i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach i jednostkach organizacyjnych powiatu.

.....

Wydział/

jednostka organizacyjna

Rejestr ryzyk / Monitorowanie/Raportowanie

Informacja (kwartalna/półroczna*)

Lp.	Cel strategiczny	Cel szczegółowy/operacyjny	Ryzyko	Poziom istotności ryzyka	Czy doszło do zmian w poziomie ryzyka (jeżeli tak wskazać nowy poziom)		Zaplanowane działania w celu obniżenia ryzyka	Jakie zrealizowano działania mające na celu obniżenie ryzyka oraz czy podjęte działania są skuteczne? **(zaznaczyć skuteczne/nieskuteczne)**		Właściciel ryzyka
1	2	3	4	5	6		7	8	9	10
					Tak/Nie	Poziom		Zrealizowane działania	Skuteczne/nieskuteczne	
							1. 2. 3.			
							1. 2. 3.			
							1. 2.			
							1. 2.			

.....

Data

.....

Podpis dyrektora

Akceptujący:

.....

*niewłaściwe skreślić

Załącznik Nr 8 do Zasad
funkcjonowania oraz metod monitorowania i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach i jednostkach organizacyjnych powiatu.

.....

Wydział/

jednostka organizacyjna

Sprawozdanie z realizacji najważniejszych celów Starostwa/ jednostki organizacyjnej powiatu za okres sprawozdawczy (półroczny/roczny).....

Część A: Realizacja najważniejszych celów

Lp..	Cel strategiczny	Cel szczegółowy/operacyjny	Termin realizacji celu/zadań	Mierniki określające stopień realizacji celu	Wartość miernika do osiągnięcia		Planowane zadania służące realizacji celu	Podjęte/zrealizowane zadania służące realizacji celu	Uwagi: Komórka organizacyjna/osoba odpowiedzialna
					planowana	osiągnięta			
1	2	3	4	5	6	7	8	9	10

Część B: *Informacja dotycząca realizacji celów w okresie sprawozdawczym (należy krótko opisać najważniejsze przyczyny , które wpłynęły na niezrealizowanie celów; wystąpienie istotnych różnic w planowanych i osiągniętych wartościach mierników lub podjęcie innych niż planowane zadań, służących realizacji celów)*

.....
Data

.....
Podpis dyrektora

Akceptuję:

.....

Załącznik Nr 9 do Zasad
funkcjonowania oraz metod monitorowania i oceny systemu kontroli zarządczej
w Starostwie Powiatowym w Kielcach i jednostkach organizacyjnych powiatu.

Oświadczenie

o stanie kontroli zarządczej za rok .....

.....

(nazwa wydziału/ jednostki organizacyjnej powiatu)

Jako osoba odpowiedzialna za zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej, a w szczególności dla zapewnienia:

- zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi,
- skuteczności i efektywności działania,
- wiarygodności sprawozdań,
- ochrony zasobów,
- przestrzegania i promowania zasad etycznego postępowania,
- efektywności i skuteczności przepływu informacji,
- zarządzania ryzykiem,

oświadczam, iż ogół działań podjętych w kierowanym przeze mnie wydziale/ jednostce sektora finansów publicznych **zapewnia/częściowo zapewnia/nie zapewnia*** realizację/ji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

* niewłaściwe skreślić

Tabela 1

Kontrola zarządcza w wystarczającym stopniu zapewniła funkcjonowanie następujących elementów:

Lp.	Standardy kontroli zarządczej	Tak	Nie	Nie całkiem	Zastrzeżenia (w przypadku odpowiedzi nie lub nie całkiem)
A.	**Środowisko wewnętrzne**				
1.	Przestrzeganie wartości etycznych				
2.	Kompetencje zawodowe				
3.	Struktura organizacyjna				
4.	Delegowanie uprawnień				
B.	**Cele i zarządzanie ryzykiem**				
1.	Misja				
2.	Określanie celów i zadań, monitorowanie i ocena ich realizacji				
3.	Identyfikacja ryzyka				
4.	Analiza ryzyka				
5.	Reakcja na ryzyko				
C.	**Mechanizmy kontroli**				
1.	Dokumentowanie systemu kontroli zarządczej				
2.	Nadzór				
3.	Ciągłość działalności				
4.	Ochrona zasobów				
5.	Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych				
6.	Mechanizmy kontroli dotyczące systemów informatycznych				
D.	**Informacja i komunikacja**				
1.	Bieżąca informacja				
2.	Komunikacja wewnętrzna				
3.	Komunikacja zewnętrzna				
E.	**Monitorowanie i ocena**				
1.	Monitorowanie systemu kontroli zarządczej				

2.	Samoocena				
3.	Audyt wewnętrzny				
4.	Uzyskano wszystkie potrzebne dane/informacje niezbędne do zapewnienia o stanie kontroli zarządczej				

Tabela 2

Lp.	**Obszar**	**Działania, które zostały podjęte w ubiegłym roku w celu poprawy funkcjonowania kontroli zarządczej.**
A.	Środowisko wewnętrzne	
B.	Cele i zarządzanie ryzykiem	
C.	Mechanizmy kontroli	
D.	Informacja i komunikacja	
E.	Monitorowanie i ocena	

Tabela 3

Lp.	**Obszar**	**Zastrzeżenia dotyczące funkcjonowania kontroli zarządczej w roku ubiegłym**
A.	Środowisko wewnętrzne	
B.	Cele i zarządzanie ryzykiem	
C.	Mechanizmy kontroli	
D.	Informacja i komunikacja	
E.	Monitorowanie i ocena	

Tabela 4

Lp.	**Obszar**	**Planowane działania, które zostaną podjęte w celu poprawy funkcjonowania kontroli zarządczej wraz z podaniem terminu ich realizacji.**
A.	Środowisko wewnętrzne	
B.	Cele i zarządzanie ryzykiem	
C.	Mechanizmy kontroli	
D.	Informacja i komunikacja	
E.	Monitorowanie i ocena	

Niniejsze oświadczenie opiera się na mojej ocenie i informacjach dostępnych w czasie jego sporządzania pochodzących z przeprowadzonych:

- monitoringu realizacji celów i zadań,
- procesu zarządzania ryzykiem,
- audytu wewnętrznego,
- kontroli wewnętrznych
- kontroli zewnętrznych
- innych źródeł informacji:.....

....

Data *Podpis dyrektora*