

ZARZĄDZENIE Nr 16/2023
Starosty Kępińskiego
z dnia 6 kwietnia 2023r.

w sprawie ustalenia systemu kontroli zarządczej dla Starostwa Powiatowego w Kępnie i jednostek organizacyjnych Powiatu Kępińskiego.

Na podstawie art. 69 ust. 1 pkt 2 i 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2022 r. poz. 1634; ze zm.), art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2022 r. poz. 1526), w związku z Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF Nr 15, poz. 84) zarządzam, co następuje:

§ 1. Ustalam „Ogólne zasady sprawowania kontroli zarządczej dla Starostwa Powiatowego w Kępnie i jednostek organizacyjnych Powiatu Kępińskiego”, w brzmieniu załącznika Nr 1 do zarządzenia.

§ 2. Ustalam „Regulamin kontroli w jednostkach organizacyjnych Powiatu Kępińskiego”, w brzmieniu załącznika Nr 2 zarządzenia.

§ 3. Ustalam „Zasady planowania celów i zadań do realizacji oraz sporządzania sprawozdań dla Starostwa Powiatowego w Kępnie i jednostek organizacyjnych Powiatu Kępińskiego”, w brzmieniu załącznika Nr 3 do zarządzenia.

§ 4. Ustalam „Zasady dokonywania analizy ryzyka oraz ustalania sposobów reakcji na ryzyko dla Starostwa Powiatowego w Kępnie i jednostek organizacyjnych Powiatu Kępińskiego”, w brzmieniu załącznika Nr 4 do zarządzenia.

§ 5. Ustalam „Zasady dokonywania samooceny systemu kontroli zarządczej oraz udzielania informacji o stanie kontroli zarządczej dla Starostwa Powiatowego w Kępnie i jednostek organizacyjnych Powiatu Kępińskiego”, w brzmieniu Załącznika Nr 5 do niniejszego zarządzenia.

§ 6. Tracą moc :

- 1) zarządzenie nr **6/15** Starosty Kępińskiego z dnia 16 lutego 2015 r. w sprawie wprowadzenia „Regulaminu kontroli zarządczej i wewnętrznej”;
- 2) zarządzenie nr **7 /2015** Starosty Kępińskiego z dnia 17 lutego 2015 r. w sprawie: systematyzowania systemu kontroli zarządczej w Starostwie Powiatowym w Kępnie w jednostkach organizacyjnych Powiatu Kępińskiego oraz w powiatowych służbach, inspekcjach i strażach;
- 3) zarządzenie nr **8 /2015** Starosty Kępińskiego z dnia 18 lutego 2015 r. w sprawie: Instrukcji Samooceny o Stanie Kontroli Zarządczej w Starostwie Powiatowym w Kępnie;
- 4) zarządzenie nr **9/2015** Starosty Kępińskiego z dnia 23 lutego 2015 r. w sprawie: Polityki Zarządzania Ryzykiem.

§ 7. Wykonanie zarządzenia powierzam Sekretarzowi Powiatu Kępińskiego.

§ 8. Zarządzenie wchodzi w życie z dniem podpisania.

**OGÓLNE ZASADY SPRAWOWANIA KONTROLI ZARZĄDCZEJ DLA STAROSTWA
POWIATOWEGO W KĘPNIE I JEDNOSTEK ORGANIZACYJNYCH POWIATU
KĘPIŃSKIEGO**

§ 1. Ustalone niniejszym dokumentem ogólne zasady sprawowania kontroli zarządczej mają zastosowanie do Starostwa Powiatowego w Kępnie i wszystkich jednostek organizacyjnych Powiatu Kępińskiego.

§ 2. 1. Kontrolę zarządczą w Starostwie Powiatowym w Kępnie oraz jednostce samorządu terytorialnego, jaką jest Powiat Kępiński stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

2. Celem kontroli zarządczej jest zapewnienie w szczególności:

- 1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi;
- 2) skuteczności i efektywności działania;
- 3) wiarygodności sprawozdań;
- 4) ochrony zasobów;
- 5) przestrzegania i promowania zasad etycznego postępowania;
- 6) efektywności i skuteczności przepływu informacji;
- 7) zarządzania ryzykiem.

3. Kontrola zarządcza to system mechanizmów, zasad i narzędzi służących zarządzaniu jednostką i osiągnięciu przez nią ustalonych celów.

§ 3. 1. Zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej w Powiecie Kępińskim, jako jednostce samorządu terytorialnego, należy do obowiązków Przewodniczącego Zarządu Powiatu Kępińskiego.

2. Zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej w jednostce organizacyjnej należy do kierownika jednostki.

§ 4. 1. Kontrola zarządcza w Starostwie Powiatowym w Kępnie oraz we wszystkich jednostkach organizacyjnych Powiatu Kępińskiego jest realizowana z zastosowaniem standardów kontroli zarządczej dla sektora finansów publicznych ogłoszonych Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. (Dz. Urz. MF z 2009 r. Nr 15 poz. 84).

2. System kontroli zarządczej obejmuje:

- 1) środowisko wewnętrzne;
- 2) cele i zarządzanie ryzykiem;
- 3) mechanizmy kontroli;
- 4) informację i komunikację;
- 5) monitorowanie i ocenę.

3. Szczegółowe zalecenia jakościowe dotyczące systemu kontroli zarządczej, określa załącznik do ogólnych zasad sprawowania kontroli zarządczej.

§ 5.1. W celu sprawnego funkcjonowania Starostwa Powiatowego w Kępnie i wszystkich jednostek organizacyjnych Powiatu Kępińskiego oraz prawidłowej realizacji zadań powiatu, kierownicy jednostek oraz naczelnicy wydziałów starostwa są obowiązani podejmować działania w kierunku właściwego przygotowania organizacyjnego jednostki lub wydziału do realizacji zadań oraz właściwego przygotowania merytorycznego jej pracowników.

2. System zarządzania jednostką/wydziałem obejmuje procedury wewnętrzne, etykę zawodową, sposób komunikowania się z klientami wewnętrznymi i zewnętrznymi, poziom

kompetencji pracowników, nabór pracowników, podnoszenie kompetencji zawodowych a także precyzyjne określanie poszczególnym pracownikom właściwego zakresu odpowiedzialności i uprawnień.

§ 6. 1. Każda jednostka organizacyjna ma jasno określony cel swojego istnienia oraz ustalone zadania do realizacji, zawarte w statutach i regulaminach organizacyjnych.

2. Cele do osiągnięcia i zadania do realizacji w ujęciu wieloletnim są wskazane w programach wieloletnich, w szczególności w strategii rozwoju powiatu i innych strategiach szczegółowych, wieloletniej prognozie finansowej oraz innych planach i programach.

3. Zadania do realizacji w roku budżetowym ujęte są w uchwale budżetowej.

4. Realizacja zadań o szczególnym znaczeniu dla powiatu jest na bieżąco monitorowana i nadzorowana.

5. Dla zwiększenia prawdopodobieństwa osiągnięcia celów i zrealizowania zaplanowanych zadań w każdej jednostce organizacyjnej powiatu oraz w każdym wydziale starostwa powiatowego są definiowane ryzyka, które mogłyby zakłócić prawidłową realizację zadań.

§ 7. 1. Kierownik każdej jednostki organizacyjnej powiatu jest odpowiedzialny za wdrożenie i funkcjonowanie systemu kontroli zarządczej w jednostce oraz ustalenie mechanizmów kontroli w postaci przepisów wewnętrznych, procedur, zarządzeń, instrukcji, zakresów czynności, sposobów postępowania.

2. System kontroli zarządczej powinien być dostosowany do potrzeb danej jednostki.

3. Dokumentacja systemu powinna być spójna i dostępna dla wszystkich pracowników, dla których jest niezbędna.

4. Wszystkie mechanizmy (ustalone procedury postępowania) powinny być jasne i proste, by ich stosowanie i przestrzeganie nie było utrudnione, czy zbyt skomplikowane.

5. Należy prowadzić nadzór nad wykonaniem zadań w celu ich oszczędnej, efektywnej i skutecznej realizacji.

6. Należy zapewnić utrzymanie ciągłości działalności każdej jednostki.

7. Należy zadbać, aby dostęp do zasobów jednostki miały wyłącznie upoważnione osoby.

8. Ze szczególnym uwzględnieniem należy nadzorować i monitorować operacje finansowe i gospodarcze poprzez:

a) rzetelne i pełne ich dokumentowanie i rejestrowanie,

b) zatwierdzanie (autoryzację) operacji finansowych przez kierownika jednostki,

c) podział kluczowych obowiązków,

d) weryfikację operacji finansowych i gospodarczych przed i po realizacji.

9. Kierownik każdej jednostki organizacyjnej ma obowiązek określić mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych.

§ 8. 1. Osoby zarządzające i pracownicy każdej jednostki organizacyjnej powinni mieć zapewniony stały dostęp do informacji niezbędnych do wykonywania obowiązków służbowych.

2. System komunikacji w jednostce powinien umożliwiać przepływ potrzebnych informacji wewnątrz jednostki, jak również wymianę ważnych informacji z podmiotami zewnętrznymi.

3. Efektywny system komunikacji powinien zapewnić nie tylko przepływ informacji, ale także ich właściwe zrozumienie przez odbiorców.

§ 9. 1. System kontroli zarządczej w jednostce organizacyjnej powinien podlegać bieżącemu monitorowaniu i ocenie.

2. Zidentyfikowane w jednostce problemy (ryzyka) należy rozwiązywać na bieżąco.

3. Wszystkie informacje zewnętrzne (skargi, zalecenia kontroli zewnętrznych) oraz wszystkie informacje wewnętrzne, m.in. wyniki skuteczności procesów realizowanych w jednostce, problemy w działalności bieżącej jednostki, wyniki stosowanych procedur

kontrolnych (np. inwentaryzacji), dane ze sprawozdań itp. powinny być poddawane dogłębnej analizie z punktu widzenia prawidłowego funkcjonowania systemu kontroli zarządczej.

STAROSTA KĘPIŃSKI

/-/ ROBERT KIERUZAL

**Załącznik do ogólnych zasad
sprawowania kontroli zarządczej**

Zalecenia tworzenia i rozwoju systemu kontroli zarządczej*

Lp.	Standard	Zalecenia jakościowe	Przykłady zalecanych praktyk
Środowisko wewnętrzne			
1.	Przestrzeganie wartości etycznych	<p>a. Określono standardy etycznego postępowania stosowane przez osoby zarządzające i pozostałych pracowników.</p> <p>b. Określono zasady zapewnienia zgodności oraz zasady przeciwdziałania korupcji.</p> <p>c. Procedury i wytyczne kontroli zarządczej koncentrują się na zapewnieniu świadomości pracowników w zakresie wartości etycznych i ich przestrzegania przy podejmowaniu decyzji i wykonywaniu powierzonych zadań.</p> <p>d. Procedury i wytyczne uwzględniają, wspieranie przez osoby zarządzające powinny promowania przestrzeganie wartości etycznych, dając dobry przykład codziennym postępowaniem i podejmowanymi decyzjami.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Kodeks etycznego postępowania <input type="checkbox"/> Regulamin pracy <input type="checkbox"/> Procedury zapewnienia zgodności <input type="checkbox"/> Procedury antykorupcyjne, w tym przyjmowania prezentów i korzyści. <input type="checkbox"/> Rejestr korzyści. <input type="checkbox"/> Procedury przyjmowania zgłoszeń o nieprawidłowościach i ochrony sygnalistów <input type="checkbox"/> Szkolenia z obszaru etyki oraz przeciwdziałania nadużyciom i korupcji <input type="checkbox"/> Procedury postępowania dyscyplinarnego
2.	Kompetencje zawodowe pracowników	<p>a. Ustanowiona została procedura rekrutacji oraz zawarto w niej mechanizmy kontrolne konieczne do obiektywnego wyboru najlepszego kandydata na dane stanowisko pracy.</p> <p>b. Osoby zarządzające i pozostali pracownicy posiadają wiedzę, umiejętności i doświadczenie pozwalające skutecznie i efektywnie wypełniać powierzone zadania.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Procedury naboru pracowników <input type="checkbox"/> Plan szkolenia pracowników/plan rozwoju zawodowego <input type="checkbox"/> Platforma e-learningowa <input type="checkbox"/> Zakresy czynności pracowników/opis stanowiska pracy

		<p>c. Istnieje system zbierania informacji na temat potrzeb szkoleniowych i ich realizacji oraz stworzono mechanizmy zapewniające możliwość rozwoju kompetencji zawodowych pracowników jednostki.</p> <p>d. Pracownicy posiadają zakresy czynności oraz zawarto w nich mechanizmy pozwalające zapewnić adekwatność zakresów czynności pracowników.</p>	<p>Procedury okresowej oceny pracowników</p>
3.	Struktura organizacyjna	<p>a. Struktura organizacyjna jest dostosowana do aktualnych celów i zadań</p> <p>b. Zakres zadań, uprawnień i odpowiedzialności, w tym poszczególnych komórek organizacyjnych oraz aktualny zakres obowiązków, uprawnień i odpowiedzialności każdego pracownika jest określony w formie pisemnej w</p>	<p><input type="checkbox"/> Statut</p> <p><input type="checkbox"/> Regulamin organizacyjny</p> <p><input type="checkbox"/> Mapa procesów</p>
		<p>sposób przejrzysty i spójny.</p> <p>c. Regulamin organizacyjny oraz zakresy czynności pracowników są poddawane cyklicznym przeglądom.</p>	
4.	Właściwe delegowanie uprawnień	<p>a. Określenie zakresu uprawnień delegowanych poszczególnym osobom kierującym komórkami organizacyjnymi lub pozostałym pracownikom, przy czym zakres delegowanych uprawnień powinien być odpowiedni do wagi podejmowanych decyzji, stopnia ich skomplikowania i ryzyka z nimi związanego.</p> <p>b. Delegowanie uprawnień do podejmowania decyzji wraz z odpowiedzialnością za podjęte decyzje na jak najniższy akceptowalny poziom.</p> <p>c. Przekazanie uprawnień w formie odrębnego imiennego upoważnienia albo wskazania w regulaminie organizacyjnym jednostki.</p> <p>d. Prowadzenie zbiorczego rejestru wydanych pełnomocnictw i upoważnień.</p>	<ul style="list-style-type: none"> ▪ Procedury delegowania zadań/udzielania upoważnień i pełnomocnictw ▪ Określenie limitów decyzji finansowych oraz zarządczych ▪ Rejestr pełnomocnictw i upoważnień
Cele i zarządzanie ryzykiem			
5.	Określenie misji	<p>a. Określona została misja, która stanowi wsparcie w ustaleniu hierarchii celów i zadań oraz efektywnemu zarządzaniu ryzykiem.</p> <p>b. Misja stanowi krótki i syntetyczny opis celu istnienia i jest publicznie dostępna.</p>	<ul style="list-style-type: none"> ▪ Pisemna misja ▪ Publikacja misji w sposób dostępny dla pracowników i podmiotów zewnętrznych

6.	Określenie celów i zadań oraz monitorowanie i ocena ich realizacji	<ul style="list-style-type: none"> a. Na podstawie misji są formułowane cele strategiczne i operacyjne. b. Cele uwzględniają różne perspektywy działania: <ul style="list-style-type: none"> ▪ Oczekiwania interesariuszy; ▪ Możliwości poprawy sytuacji finansowej; ▪ Możliwości usprawniania procesów wewnętrznych; <input type="checkbox"/> Działania rozwojowe i innowacyjne. c. Ustalane cele i zadania są spójne ze sobą oraz z dokumentami o charakterze strategicznym. d. Określając cele i zadania wskazano komórki organizacyjne lub osoby odpowiedzialne bezpośrednio za ich wykonanie. e. Cele podlegają okresowemu monitorowaniu. f. Cele stanowią podstawę do identyfikacji, analizy ryzyka oraz doboru mechanizmów kontroli. 	<input type="checkbox"/> Udokumentowany plan działalności
7.	Identyfikacja ryzyka	<ul style="list-style-type: none"> a. Punkt wyjścia do identyfikacji ryzyka stanowi system wyznaczania i osiągnięcia celów. b. Ryzyka identyfikuje się na każdym poziomie struktur organizacyjnych c. Identyfikując ryzyka uwzględnia się kluczowe zagrożenia, które mogą negatywnie wpłynąć na osiągnięcie celów, co nie stoi w przeszkodzie identyfikacji szans i możliwości. d. Identyfikacja ryzyka stanowi, w miarę możliwości, działanie zespołowe. e. Każde ryzyko ma swojego właściciela, czyli osobę odpowiedzialną za zarządzanie ryzykiem. 	<ul style="list-style-type: none"> a. Metodyka zarządzania ryzykiem b. Rejestr ryzyka
8.	Analiza ryzyka	<ul style="list-style-type: none"> a. Analizując ryzyko ocenia się jego skutki (wpływ na cele) oraz prawdopodobieństwo. b. Ocena ryzyka ma charakter ilościowy. c. Wyniki analizy ujawnia się w rejestrze ryzyka. 	
9.	Reakcja na ryzyko	<ul style="list-style-type: none"> a. W reakcji na ryzyko można przyjąć jedną z poniższych strategii: <ul style="list-style-type: none"> <input type="checkbox"/> unikanie ryzyka - świadoma decyzja o nieangażowaniu się lub odejściu od ryzyka, działanie w celu eliminacji narażenia na konkretne ryzyko; 	

		<ul style="list-style-type: none"> <input type="checkbox"/> ograniczanie ryzyka - polega na podjęciu działań mających na celu minimalizację prawdopodobieństwa lub wpływu wystąpienia ryzyka lub obu jednocześnie, poprzez zwiększenie skuteczności stosowanych mechanizmów kontroli lub wdrożenie nowych; <input type="checkbox"/> dzielenie się ryzykiem - ograniczenie prawdopodobieństwa i wpływu wystąpienia danego ryzyka poprzez przekazanie w całości lub częściowo innej stronie, np. zawierając umowę ubezpieczenia lub inną umowę z podmiotem zewnętrznym; <input type="checkbox"/> akceptacja ryzyka - niepodjęcie dodatkowych działań w odpowiedzi na ryzyko w sytuacji, gdy ryzyko jest zarządzane w sposób wystarczający. 	
Mechanizmy kontrolne			
10.	Dokumentowanie systemu kontroli zarządczej	<ul style="list-style-type: none"> a. Dokumentacja systemu kontroli zarządczej obejmuje procedury wewnętrzne, instrukcje, wytyczne, dokumenty określające zakres obowiązków, uprawnień i odpowiedzialności pracowników i inne dokumenty wewnętrzne oraz rejestr obowiązujących przepisów wewnętrznych; b. Dokumentacja systemu kontroli zarządczej jest dostępna dla wszystkich osób, dla których jest niezbędna; c. Dokumentacja systemu kontroli zarządczej jest na bieżąco aktualizowana 	<ul style="list-style-type: none"> <input type="checkbox"/> Wykaz regulacji wewnętrznych <input type="checkbox"/> Akta spraw <input type="checkbox"/> Zapisy w systemach IT <input type="checkbox"/> Pisemne potwierdzenie wykonywanych weryfikacji, zatwierdzeń i stosowania mechanizmów kontroli
11.	Nadzór nad wykonywaniem zadań	<ul style="list-style-type: none"> a. Wprowadzono nadzór nad wykonaniem zadań w celu ich oszczędnej, efektywnej i skutecznej realizacji, z uwzględnieniem właściwego sposobu podziału zadań i odpowiedzialności oraz zakresu decyzji możliwych do podjęcia przez poszczególne osoby 	<ul style="list-style-type: none"> <input type="checkbox"/> Instruktaż stanowiskowy pracownika <input type="checkbox"/> Weryfikacja i zatwierdzanie działań <input type="checkbox"/> Informacja zwrotna przełożonego do pracownika o sposobie wykonania zadania <input type="checkbox"/> Praktyki określone w standardach obejmujących cele i zarządzanie ryzykiem oraz monitorowanie i ocena
12.	Zapewnienie ciągłości działania	<ul style="list-style-type: none"> a. Wdrożenie mechanizmów kontrolnych zapobiegających zdarzeniom, które mogą spowodować zatrzymanie działalności - w ramach przeprowadzanej analizy ryzyka należy również uwzględnić tego typu zdarzenia. 	<ul style="list-style-type: none"> <input type="checkbox"/> Procedury ciągłości działania <input type="checkbox"/> Procedury/plany zastępstw <input type="checkbox"/> Plany działalności systemów informatycznych

		<p>b. Zostały wskazane osoby zastępujące każdego z pracowników w przypadku jego nieobecności.</p> <p>c. Zostały wskazane osoby zastępujące poszczególne osoby zarządzające podczas ich nieobecności.</p>	<p><input type="checkbox"/> Tworzenie kopii zapasowych</p> <p><input type="checkbox"/> Zapisy w umowach z dostawcami energii, mediów, usług informatycznych i</p>
		d. Opracowany został plan bezpieczeństwa na wypadek przerw w działaniu systemów informatycznych.	telekomunikacyjnych
13.	Ochrona zasobów (niefinansowych)	<p>a. Dostęp do zasobów mają jedynie upoważnione osoby.</p> <p>b. Określono odpowiedzialność kierującym komórkami organizacyjnymi i pozostałym pracownikom za zapewnienie ochrony i właściwe wykorzystanie zasobów jednostki.</p> <p>c. Weryfikowanie czy dostęp do poszczególnych zasobów, w tym m.in. do danych osobowych jest limitowany oraz przypisany do właściwych osób, z uwzględnieniem wyników analizy i oceny ryzyka w tym zakresie.</p> <p>d. Zapewnione zostało bezpieczeństwo fizyczne obiektów, w tym przeciwpożarowe. e. Istnieją i są stosowane zasady BHiP.</p>	<p><input type="checkbox"/> Procedury zapewnienia zgodności.</p> <p><input type="checkbox"/> Procedury cyberbezpieczeństwa</p> <p><input type="checkbox"/> Procedury zarządzania bezpieczeństwem informacji</p> <p><input type="checkbox"/> Polityki i procedury bezpieczeństwa teleinformatycznego</p> <p><input type="checkbox"/> Procedury ochrony danych osobowych Instrukcja bezpieczeństwa przeciwpożarowego</p> <p><input type="checkbox"/> Procedury BHiP</p> <p><input type="checkbox"/> Procedury ochrony informacji prawnie chronionych</p>
14.	Mechanizmy kontroli dotyczące operacji gospodarczych i finansowych	<p>a. Zaciąganie zobowiązań w granicach określonych w planie finansowym.</p> <p>b. Ustalenie limitów do podejmowania decyzji finansowych i gospodarczych przez upoważnione osoby.</p> <p>c. Rzetelne i pełne dokumentowanie i rejestrowanie operacji finansowych i gospodarczych.</p> <p>d. Weryfikacja operacji finansowych i gospodarczych z zastosowaniem zasady wielu par oczu.</p> <p>e. Zatwierdzanie (autoryzacja) operacji finansowych i gospodarczych przez kierownika jednostki lub osoby przez niego upoważnione.</p> <p>f. Weryfikacja wykonawcy, dostawcy oraz kontrahenta pod kątem wykonalności umowy oraz zabezpieczenia przed ryzykiem korupcji.</p> <p>g. Zabezpieczenie interesów jednostki w zawieranych umowach.</p> <p>h. Opiniowanie projektów umów przez radcę prawnego.</p>	<p><input type="checkbox"/> Plany finansowe</p> <p><input type="checkbox"/> Polityka rachunkowości</p> <p><input type="checkbox"/> Instrukcja obiegu dokumentacji finansowo-księgowej</p> <p><input type="checkbox"/> Procedury przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu</p> <p><input type="checkbox"/> Procedury windykacji i egzekucji należności</p> <p><input type="checkbox"/> Procedury rozliczania delegacji służbowych</p> <p><input type="checkbox"/> Procedury udzielania zamówień publicznych, w tym weryfikacji kontrahentów</p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p>

		i. Ograniczenie stosowania płatności gotówkowych w związku z wykonywanymi operacjami finansowymi i gotówkowymi.	Wykaz zawieranych umów Legalne i na bieżąco aktualizowany system finansowo-księgowy.
15.	Mechanizmy kontroli dotyczące systemów informatycznych	<p>a. Mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych, obejmują m.in. mechanizmy kontroli dostępu do zasobów informatycznych, mające na celu ich ochronę przed nieautoryzowanymi zmianami, utratą lub ujawnieniem.</p> <p>b. Stosowane jest licencjonowane i regularnie aktualizowane oprogramowanie.</p> <p>c. Istnieją mechanizmy kontroli oprogramowania systemowego.</p> <p>d. Stan infrastruktury sieciowej jest adekwatny do potrzeb jednostki.</p> <p>e. Dokonuje się regularnych audytów systemów informatycznych</p>	<input type="checkbox"/> Standardy budowy i rozwoju infrastruktury sieciowej <input type="checkbox"/> Wykaz aktywów w systemach teleinformatycznych <input type="checkbox"/> Wykaz licencjonowanego oprogramowania i aplikacji <input type="checkbox"/> Praktyki z obszaru standardu ochrona zasobów

Informacja i komunikacja			
16.	Bieżąca informacja	<p>a. Osoby zarządzające, jak i pozostali pracownicy posiadają, w odpowiedniej formie i czasie, dostęp do właściwych oraz rzetelnych informacji potrzebnych do realizacji zadań.</p> <p>b. Każdy z pracowników posiadają dostęp do informacji, które są przez niego wykorzystywane w codziennej pracy.</p> <p>c. Przeprowadzana jest analiza ryzyka w zakresie informacji dostępnych dla poszczególnych osób ze szczególnym zwróceniem uwagi na stosowane mechanizmy kontroli.</p>	<input type="checkbox"/> Instrukcja kancelaryjna/obiegu dokumentacji <input type="checkbox"/> Zabezpieczona strona internetowa. Intranet do przekazywania informacji wewnątrz organizacji. <input type="checkbox"/> Aktualny spis numerów telefonów i adresów poczty elektronicznej. <input type="checkbox"/> Aktualny Biuletyn Informacji Publicznej. <input type="checkbox"/> Procedury udzielania informacji publicznej Procedury przyjmowania i rozpatrywania skarg i wniosków. <input type="checkbox"/> Procedury przyjmowania zgłoszeń o nieprawidłowościach i ochrony sygnalistów.
17	Komunikacja wewnętrzna	<p>a. Istnieją efektywne mechanizmy przekazywania ważnych informacji w obrębie struktury organizacyjnej.</p> <p>b. Pracownicy posiadają konieczną wiedzę na temat organizacji jednostki organizacyjnej i jej funkcjonowania w zakresie realizowanych obowiązków,</p> <p>c. Informacje na temat kluczowych problemów i ryzyk oraz stosowanych mechanizmów kontroli są przekazywane w określony sposób oraz w ustalonym czasie i formie.</p>	

18.	Komunikacja zewnętrzna	<p>a. W pierwszej kolejności na zewnątrz są przekazywane informacje wymagane przepisami prawa.</p> <p>b. Informacji są przekazywane przekazywanych na zewnątrz w formie określonej w procedurach (np. za pośrednictwem Biuletynu Informacji Publicznej, strony internetowej jednostki, przez rzecznika prasowego).</p>	Księga stylu.
Monitorowanie i ocena			
19.	Monitorowanie systemu kontroli zarządczej oraz celów i zadań	<p>a. Wszystkie elementy systemu kontroli zarządczej są przeglądane.</p> <p>b. Dane w zakresie analizy ryzyka i możliwości realizacji na ich podstawie działań w zakresie postępowania z kluczowymi ryzykami są aktualizowane.</p>	<input type="checkbox"/> Rejestr kontroli zewnętrznych <input type="checkbox"/> Rejestr zaleceń audytowych i wniosków pokontrolnych <input type="checkbox"/> Rejestr skarg i wniosków <input type="checkbox"/> Rejestr zgłoszeń o nieprawidłowościach <input type="checkbox"/> Mapa zapewnienia <input type="checkbox"/> Sprawozdanie z planu działalności <input type="checkbox"/> Kwestionariusz pytań samooceny kontroli zarządczej <input type="checkbox"/> Oświadczenie o stanie kontroli zarządczej
20.	Samoocena kontroli zarządczej	<p>a. Samoocena dokonywana jest z użyciem anonimowych formularzy ankietowych uwzględniających ocenę wszystkich standardów kontroli zarządczej oraz specyfikę działania jednostki.</p> <p>b. Podsumowanie wyników samooceny uwzględnia w szczególności ogólną ocenę funkcjonowania systemu kontroli zarządczej, zidentyfikowane słabości systemu kontroli zarządczej oraz proponowane działania naprawcze.</p>	
21.	Audyt wewnętrzny	<p>a. Nowego ryzyka dotychczas nieujętych w rejestrze ryzyka są identyfikowane.</p> <p>b. Oceniana jest skuteczności stosowanych mechanizmów kontroli ryzyka.</p> <p>c. Oceniana jest skuteczności działań podejmowanych w odniesieniu do ryzyk, uznanych za krytyczne.</p> <p>d. Doskonalone są procesy zarządzania ryzykiem.</p>	<input type="checkbox"/> Karta audytu wewnętrznego <input type="checkbox"/> Procedury audytu wewnętrznego <input type="checkbox"/> Rejestr zaleceń audytowych

22.	Uzyskanie zapewnienia o stanie kontroli zarządczej	Źródłem uzyskania zapewnienia o stanie kontroli zarządczej przez kierownika jednostki powinny być w szczególności wyniki: monitorowania, samooceny oraz przeprowadzonych audytów i kontroli. Zaleca się coroczne potwierdzenie uzyskania powyższego zapewnienia w formie oświadczenia o stanie kontroli zarządczej za poprzedni rok.	Oświadczenia o stanie kontroli zarządczej składane według zasad określonych treścią niniejszego Zarządzenia. Por. Załącznik nr 3 do zarządzenia por. § 5 ust. 1 Załącznika nr 3 do zasad planowania celów i zadań do realizacji oraz sporządzania sprawozdań dla Starostwa Powiatowego w Kępnie i jednostek organizacyjnych Powiatu Kępińskiego.
-----	---	--	--

*Powyższe zalecenia jakościowe i praktyki określają przykładowe rekomendowane, a nie obligatoryjne wskazówki w ramach tworzenia i rozwijania systemu. Kierownik jednostki organizacyjnej może podejmować decyzje o stosowaniu innych praktyk, które określają sposób realizacji danego standardu kontroli zarządczej w podległej jednostce. Zalecenia stanowią wytyczne do oceny systemu kontroli zarządczej przez funkcję audytu wewnętrznego.

REGULAMIN KONTROLI W JEDNOSTKACH ORGANIZACYJNYCH POWIATU KĘPIŃSKIEGO

§ I. Kontrole przeprowadzane w jednostkach organizacyjnych Powiatu Kępińskiego stanowią element sprawowanej kontroli zarządczej.

§ 2.1. Kontrole w jednostkach organizacyjnych powiatu są przeprowadzane dla zapewnienia, że cele i zadania jednostek są realizowane w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

2. Celem przeprowadzanych kontroli w jednostkach jest sprawdzenie:

- 1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi;
- 2) skuteczności i efektywności działania;
- 3) wiarygodności sprawozdań;
- 4) ochrony zasobów;
- 5) przestrzegania i promowania zasad etycznego postępowania;
- 6) efektywności i skuteczności przepływu informacji;
- 7) zarządzania ryzykiem.

3. Kontroli podlega:

- 1) zgodność dokonywanych wydatków z celami i w wysokościach ustalonych w planie finansowym jednostki;
- 2) przestrzeganie zasady uzyskiwania najlepszych efektów z danych nakładów;
- 3) przestrzeganie zasady optymalnego doboru metod i środków służących osiągnięciu założonych celów;
- 4) dokonywanie wydatków w sposób umożliwiający terminową realizację zadań;
- 5) dokonywanie wydatków w wysokościach i terminach wynikających z wcześniej zaciągniętych zobowiązań.

4. Kontrola może być prowadzona jako:

- 1) kontrola kompleksowa obejmująca całość działalności kontrolowanej jednostki;
- 2) kontrola problemowa — obejmująca wybrane zagadnienia z działalności kontrolowanej jednostki;
- 3) kontrola planowa — prowadzona zgodnie z ustalonym planem kontroli na dany rok;
- 4) kontrola doraźna — mająca charakter interwencyjny, wynikający z potrzeby pilnego zbadania wybranych operacji lub czynności;
- 5) kontrola sprawdzająca — mająca na celu zbadanie wykonania zaleceń pokontrolnych.

§ 3. Kontrole w jednostkach podległych Powiatowi Kępińskiemu przeprowadzane są przez osobę lub zespół kontrolny wyznaczony przez Starostę Kępińskiego.

§4.1. Kontrole przeprowadzane są na podstawie imiennego upoważnienia Starosty Kępińskiego, w którym zostaje wskazana jednostka kontrolowana, podstawa przeprowadzenia kontroli, rodzaj i przedmiot oraz termin przeprowadzenia kontroli.

2. Upoważnienie do przeprowadzenia kontroli wystawiane jest w trzech egzemplarzach: dla komórki kontrolowanej, do rejestru upoważnień oraz do akt kontroli.

§ 5. I . Plan kontroli, o których mowa w § 2 pkt 1 i 2 jest opracowywany przez Sekretarza Powiatu w pierwszym kwartale roku, którego dotyczy.

2.Plan kontroli zatwierdza Starosta Kępiński.

3.Plan kontroli określa:

- 1) jednostkę kontrolowaną;
- 2) rodzaj i przedmiot kontroli;
- 3) planowany termin kontroli.

4. Przy opracowywaniu planu, o którym mowa w ust. 1 uwzględnia się w szczególności:

- 1) zadania wynikające z przepisów prawa;
- 2) wyniki wcześniejszych kontroli;
- 3) wyniki badań i analiz określonych problemów oraz skarg i wniosków.

§ 6. I . Kontrolujący, przed rozpoczęciem czynności kontrolnych, przekazuje kierownikowi jednostki kontrolowanej upoważnienie do przeprowadzenia kontroli oraz dokonuje wpisu do książki kontroli prowadzonej przez jednostkę kontrolowaną.

2. W czasie wykonywania czynności kontrolnych, kontrolujący ma prawo do:

- 1) swobodnego poruszania się na terenie jednostki kontrolowanej;
- 2) wglądu do dokumentów i materiałów dotyczących przedmiotu kontroli;
- 3) wykonania kserokopii dokumentów, zgodnie z obowiązującymi przepisami o ochronie tajemnicy służbowej;
- 4) żądania udzielania ustnych lub pisemnych wyjaśnień;
- 5) przeprowadzania oględzin obiektów i innych składników majątkowych.

3. W celu sprawnego i rzetelnego przeprowadzenia kontroli kierownik jednostki kontrolowanej jest obowiązany do:

- 1) zapewnienia kontrolującemu odpowiedniego pomieszczenia oraz wyposażenia do prowadzenia czynności kontrolnych oraz przechowywania materiałów kontrolnych;
- 2) udostępniania żądanych dokumentów dotyczących przedmiotu kontroli;
- 3) umożliwienia dokonania oględzin;
- 4) zobowiązania pracowników do udzielania wyjaśnień;
- 5) składania ustnych i pisemnych wyjaśnień dotyczących przedmiotu kontroli.

4. W trakcie trwania kontroli do obowiązków pracowników jednostki kontrolowanej należy:

- 1) przygotowanie na potrzeby kontrolującego niezbędnych zestawień i obliczeń, kserokopii dokumentów;
- 2) składanie ustnych i pisemnych wyjaśnień w sprawach dotyczących przedmiotu kontroli;
- 3) uczestniczenie w czynnościach kontrolnych w niezbędnym zakresie (np. podczas kontroli kasy i magazynu — osoby odpowiedzialne materialnie).

§ 7. 1 . Kontrolujący podlega wyłączeniu z kontroli na wniosek lub z urzędu, jeżeli wyniki kontroli mogą dotyczyć jego praw lub obowiązków albo praw lub obowiązków jego małżonka lub osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnych i powinowatych do drugiego stopnia albo osób związanych z nim z tytułu przysposobienia, opieki lub kurateli. Powody wyłączenia kontrolującego trwają mimo ustania małżeństwa, wspólnego pożycia, przysposobienia, opieki lub kurateli.

2. Kontrolujący podlega wyłączeniu również w razie zaistnienia w toku kontroli okoliczności mogących

wywołać uzasadnione wątpliwości, co do jego bezstronności. Wniosek do Starosty o wyłączenie z kontroli może złożyć kontrolujący lub kierownik jednostki kontrolowanej.

3.W okresie od złożenia wniosku do wyłączenia z kontroli, kontrolujący podejmuje wyłącznie czynności niecierpiące zwłoki.

4. Ustalenia kontrolującego, który został wyłączony z kontroli, z zastrzeżeniem ust. 4, nie są uwzględniane w protokole kontroli.

5. O wyłączeniu kontrolującego z kontroli decyduje Starosta Kępiński.

§ 8. I . Kontrolujący dokonuje ustaleń na podstawie dowodów, do których zalicza się: dokumenty, dowody rzeczowe, protokoły z oględzin, dane ewidencji i sprawozdawczości, opinie specjalistów i biegłych, zdjęcia, szkice, oświadczenia, zastrzeżenia i wyjaśnienia złożone na piśmie przez kierownika jednostki kontrolowanej oraz pracowników odpowiedzialnych za powierzony odcinek pracy.

2. Kserokopie dokumentów potwierdzone za zgodność z oryginałem przez kierownika jednostki kontrolowanej lub osobę przez niego upoważnioną, mogą być dołączone do protokołu kontroli.

§ 9. I . Kontrolujący jest obowiązany do bieżącego informowania kierownika jednostki kontrolowanej o ujawnionych nieprawidłowościach w jej działalności, wskazując na celowość niezwłocznego podjęcia przez niego środków zaradczych i korygujących.

2. Kierownik jednostki kontrolowanej obowiązany jest niezwłocznie poinformować kontrolującego o podjętych działaniach zapobiegających występowaniu nieprawidłowości, o których mowa w ust. I .

3. W razie ujawnienia w toku kontroli faktów i okoliczności uzasadniających podejrzenie popełnienia przestępstwa lub naruszenia dyscypliny finansów publicznych, kontrolujący zawiadamia Starostę Kępińskiego i zabezpiecza zebrane w tej sprawie materiały dowodowe.

§ 10. I . Dokonane w toku kontroli ustalenia kontrolujący opisuje w protokole kontroli, który powinien być sporządzony w terminie 30 dni po zakończeniu kontroli.

2. Protokół kontroli powinien zawierać:

- 1) oznaczenie jednostki kontrolowanej, jej siedzibę, adres, imię i nazwisko kierownika jednostki, z uwzględnieniem zmian zaistniałych w okresie objętym kontrolą;
- 2) imię i nazwisko oraz stanowisko służbowe kontrolującego oraz numer i datę upoważnienia do przeprowadzenia kontroli;
- 3) datę rozpoczęcia i zakończenia czynności kontrolnych w jednostce kontrolowanej, z wyszczególnieniem ewentualnych przerw w kontroli;
- 4) określenie przedmiotu kontroli;
- 5) oznaczenie okresu objętego kontrolą;
- 6) opis stanu faktycznego stwierdzonego w toku kontroli, a w szczególności opis nieprawidłowości z uwzględnieniem, w miarę możliwości, przyczyn ich powstania i wywołanych skutków oraz osób za nie odpowiedzialnych;
- 7) pouczenie o prawie, sposobie i terminie zgłoszenia zastrzeżeń do ustaleń zawartych w protokole kontroli oraz o prawie odmowy podpisania protokołu kontroli;
- 8) informację o liczbie egzemplarzy protokołu wraz ze wzmianką o przeznaczeniu jednego egzemplarza dla kierownika jednostki kontrolowanej ;
- 9) wykaz załączników do protokołu;
- 10) miejsce i datę podpisania protokołu kontroli przez kontrolującego;
- 11) miejsce i datę podpisania protokołu kontroli przez kierownika jednostki kontrolowanej oraz w przypadku, jeżeli kontrola obejmowała sprawy finansowe przez głównego księgowego;
- 12) wszystkie strony protokołu winny być parafowane przez kontrolującego i kierownika jednostki kontrolowanej.

3. W przypadku, gdy protokół kontroli lub jego część zawiera informacje stanowiące tajemnicę służbową, kontrolujący nadaje mu w całości lub części klauzulę tajności.

4. Przed przekazaniem protokołu kontroli, kontrolujący omawia z kierownikiem i głównym księgowym jednostki ustalenia zawarte w protokole kontroli.

§ 11. 1. Kierownik jednostki kontrolowanej podpisuje protokół w terminie 7 dni od dnia jego otrzymania.

2. W terminie 7 dni od dnia otrzymania protokołu kontroli, kierownik jednostki kontrolowanej może zgłosić umotywowane zastrzeżenia dotyczące ustaleń zawartych w protokole.

3. Umotywowane zastrzeżenia do protokołu złożone po terminie, o którym mowa w ust. 2 nie są rozpatrywane.

4. W przypadku zgłoszenia zastrzeżeń do protokołu, kontrolujący jest obowiązany do dokonania analizy zgłoszonych zastrzeżeń, a w miarę potrzeby do podjęcia dodatkowych czynności kontrolnych.

5. W przypadku uznania zgłoszonych zastrzeżeń do protokołu za zasadne, kontrolujący sporządza aneks do protokołu kontroli.

6. Jeżeli zgłoszone zastrzeżenia do protokołu nie zostaną uznane za zasadne, kontrolujący sporządza pisemną informację o nieuwzględnieniu zastrzeżeń, którą przekazuje niezwłocznie kierownikowi jednostki kontrolowanej.

7. Kierownik jednostki kontrolowanej może odmówić podpisania protokołu kontroli, składając w terminie 7 dni od dnia jego otrzymania pisemne wyjaśnienie odmowy podpisania protokołu.

8. Odmowa podpisania protokołu kontroli przez kierownika jednostki kontrolowanej nie stanowi przeszkody do sporządzenia zaleceń pokontrolnych.

§ 12. 1. Protokół z przeprowadzonej kontroli wraz z propozycją zaleceń pokontrolnych bądź informacją o braku zaleceń, kontrolujący przedkłada Staroście Kępińskiemu w terminie 7 dni po jego podpisaniu.

2. Starosta Kępiński może zwołać naradę pokontrolną w celu omówienia nieprawidłowości i uchybień opisanych w protokole kontroli oraz ustalenia dalszego postępowania.

3. Protokoły kontroli przechowuje Sekretarz Powiatu.

§ 13. 1. W razie stwierdzenia w toku kontroli nieprawidłowości i uchybień Starosta Kępiński przekazuje kierownikowi jednostki kontrolowanej zalecenia pokontrolne.

2. Zalecenia pokontrolne winny być przekazane w terminie 14 dni od dnia podpisania protokołu kontroli lub złożenia pisemnego uzasadnienia odmowy podpisania protokołu przez kierownika jednostki kontrolowanej.

3. Kierownik jednostki kontrolowanej w terminie 30 dni od dnia otrzymania zaleceń pokontrolnych zawiadamia pisemnie Starostę Kępińskiego o sposobie i terminie realizacji zaleceń pokontrolnych,

§ 14. I. W przypadku wystąpienia podejrzenia naruszenia dyscypliny finansów publicznych lub podejrzenia popełnienia przestępstwa, Starosta Kępiński podejmuje decyzję o powiadomieniu właściwego rzecznika dyscypliny finansów publicznych lub organów powołanych do ścigania przestępstw.

2. Zawiadomienie, o którym mowa w ust. 1 przygotowuje kontrolujący.

§ 15. I. Sekretarz Powiatu sporządza roczne sprawozdanie z wykonania planu kontroli oraz przeprowadzonych kontroli doraźnych.

2. W rocznym sprawozdaniu z wykonania kontroli ujęte zostają informacje o:

- 1) terminie przeprowadzenia poszczególnych kontroli;
- 2) stwierdzonych uchybieniach i nieprawidłowościach;
- 3) zgłoszonych do rzecznika finansów publicznych zawiadomieniach o ujawnionym naruszeniu dyscypliny finansów publicznych;
- 4) sformułowanych zaleceniach pokontrolnych.

3. Sprawozdanie, o którym mowa w ust. 1, Sekretarz Powiatu przedkłada Staroście Kępińskiemu w terminie do dnia 31 marca roku następnego.

4. Sprawozdanie, o którym mowa w ust. 1, przedkładane jest również Zarządowi Powiatu Kępińskiemu w terminie do końca kwietnia roku następnego.

**Załącznik nr 3 do zarządzenia
Nr 16/2023 Starosty Kępińskiego
z dnia 6 kwietnia 2023r.**

ZASADY PLANOWANIA CELÓW I ZADAŃ DO REALIZACJI

ORAZ SPORZĄDZANIA SPRAWOZDAŃ DLA STAROSTWA POWIATOWEGO W KĘPNIE I JEDNOSTEK ORGANIZACYJNYCH POWIATU KĘPIŃSKIEGO

§ 1. Ustalone niniejszym dokumentem Zasady planowania celów i zadań do realizacji mają zastosowanie w Starostwie Powiatowym w Kępnie

§ 2. 1. Cele i zadania Powiatu Kępińskiego zostały zawarte w:

- 1) ustawie z dnia 5 czerwca 1998 r. o samorządzie powiatowym, ustawach branżowych oraz przepisach wykonawczych wydanych na ich podstawie;
- 2) Statucie Powiatu Kępińskiego i Regulaminie Organizacyjnym Starostwa Powiatowego w Kępnie oraz statutach i regulaminach organizacyjnych jednostek organizacyjnych powiatu;
- 3) dokumentach o charakterze strategicznym dla Powiatu Kępińskiego, w szczególności: strategii rozwoju powiatu i innych strategiach szczegółowych oraz innych planach i programach opracowanych dla Powiatu Kępińskiego, a także programach, do realizacji, których przystąpił Powiat Kępiński;
- 4) Wieloletniej Prognozie Finansowej Powiatu Kępińskiego;
- 5) Uchwale budżetowej powiatu.

§ 3. 1. Dla zwiększenia jakości i skuteczności realizowanych zadań powiatu naczelnicy wydziałów Starostwa Powiatowego w Kępnie, wskazują na każdy rok budżetowy zadania do realizacji, wymagające szczególnego nadzorowania oraz objęcia monitorowaniem, zgodnie z załącznikiem nr 1 do niniejszych Zasad, w terminie do 1 marca każdego roku.

2. Do zadań, o których mowa w ust. 1 należy ująć m.in.:

- 1) wszystkie zadania inwestycyjne i remontowe ujęte w budżecie;
- 2) zadania wpisujące się w realizację celów zawartych w strategii powiatu lub innych dokumentów programowych;
- 3) inne zadania o szczególnym znaczeniu dla funkcjonowania i rozwoju powiatu.

§ 4. Monitorowanie osiągniętych celów i realizowanych zadań następuje podczas:

- a) monitorowania realizacji powiatowych strategii i programów wskazanych w § 2 ust. 1 pkt 3,
- b) analizy wykonania i zmian Wieloletniej Prognozy Finansowej,
- c) analizy wykonania i zmian budżetu powiatu,
- d) monitorowania realizacji zadań zaplanowanych na dany rok budżetowy.

§ 5.1. Naczelnicy wydziałów oraz pracownicy samodzielnych stanowisk Starostwa Powiatowego w Kępnie, w terminie do 20 lutego roku sporządzają za miniony rok sprawozdanie z realizacji zaplanowanych zadań oraz działalności wydziału/samodzielnego stanowiska pracy zgodnie z załącznikiem Nr 2 do niniejszych Zasad.

2. Naczelnicy wydziałów oraz pracownicy samodzielnych stanowisk Starostwa Powiatowego w Kępnie oraz kierownicy jednostek organizacyjnych Powiatu Kępińskiego, w terminie do 20 lutego roku sporządzają za miniony rok oświadczenie o stanie kontroli zarządczej zgodnie z załącznikiem nr 3 do niniejszych zasad.

3. Kierownicy jednostek organizacyjnych Powiatu Kępińskiego sporządzają sprawozdanie z działalności jednostki za miniony rok zgodnie z planem pracy Rady Powiatu Kępińskiego na dany rok.

§ 6. 1. W miesiącu marcu jest dokonywany przegląd funkcjonowania systemu kontroli zarządczej w Starostwie Powiatowym w Kępnie oraz w Powiecie Kępińskim w poprzednim roku.

2. Przegląd, o którym mowa w ust. 1 jest dokonywany przez Starostę przy współudziale Wicestarosty, Skarbnika, Sekretarza.

3. Sekretarz Powiatu Kępińskiego sporządza Informację na temat funkcjonowania systemu kontroli zarządczej w Starostwie Powiatowym w Kępnie oraz w Powiecie Kępińskim przedkłada ją Staroście w terminie do 31 marca.

4. Starosta przedkłada Informację na temat funkcjonowania systemu kontroli zarządczej w Starostwie Powiatowym w Kępnie oraz w Powiecie Kępińskim Zarządowi Powiatu Kępińskiego w terminie nie dłuższym niż do końca kwietnia.

§ 7. Sprawozdania z wykonania budżetu, Wieloletniej Prognozy Finansowej, realizacji strategii, planów i programów, o których mowa w § 2 pkt 3-5 sporządzane są zgodnie z przepisami regulującymi ich sporządzanie.

**Załącznik nr 1 do Zasad planowania celów i zadań
do realizacji oraz sporządzania sprawozdań
dla Starostwa Powiatowego w Kępnie
i jednostek organizacyjnych Powiatu Kępińskiego**

wydział /referat Urzędu/ jednostka organizacyjna

Plan działalności na rok [.....]

Lp.	Perspektywa celu¹	Opis celu²	Planowany termin realizacji³	Częstotliwość monitorowania⁴	Komórka/osoba odpowiedzialna
[1]	[2]	[3]	[4]	[5]	[6]
1.		<i>Nazwa celu</i>			
		<i>Opis kluczowego rezultatu 1</i>			
		<i>Wskazanie zadania 1 (działanie, projekt)</i>			
		<i>Wskazanie zadania 2 (działanie, projekt)</i>			
		<i>Opis kluczowego rezultatu 2</i>			
		<i>Wskazanie zadania 1 (działanie, projekt)</i>			
		<i>Wskazanie zadania 2 (działanie, projekt)</i>			

Sporządził:

Zatwierdził:

¹ Cele wyznaczone są w czterech perspektywach: 1) interesariusza zewnętrznego, 2) finansowej, 3) procesów wewnętrznych, 4) rozwoju.

² Opis każdego celu składa się z trzech elementów: 1) jakościowy opis zmiany, którą planuje się osiągnąć, 2) opis mierzalnego (ilościowego) rezultatu, który wskazuje na osiągnięcie celu, 3) planowanych działań, które przyczynią się do osiągnięcia celu i kluczowego rezultatu.

³ Cele strategiczne realizowane są w terminach co najmniej rocznych. Cele operacyjne realizowane są w terminach rocznych, półrocznych lub kwartalnych.

⁴ Częstotliwość monitorowania powinna być dostosowana do terminu realizacji celu, np. dla celów rocznych zaleca się monitorowanie kwartalne, dla celów półrocznych lub kwartalnych monitorowanie miesięczne.

**Załącznik nr 2 do Zasad planowania celów i zadań
do realizacji oraz sporządzania sprawozdań
dla Starostwa Powiatowego w Kępnie
i jednostek organizacyjnych Powiatu Kępińskiego**

wydział /referat Urzędu/ jednostka organizacyjna

Lp.	Perspektywa celu	Opis celu	Planowany termin realizacji	Stopień realizacji na dzień 31.12.	Komórka/osoba odpowiedzialna
[1]	[2]	[3]	[4]	[5]	[6]
1.		<i>Nazwa celu</i>			
		<i>Opis kluczowego rezultatu 1</i>			
		<i>Opis kluczowego rezultatu 2</i>			

Sporządził:

Zatwierdził:

Powyższa tabela sprawozdawcza winna zawierać dane dotyczące:

1. Informacje na temat ilości zrealizowanych spraw (wydane decyzje, postanowienia, pozwolenia, wypisy, wyrysy, zaświadczenia, opinie, wprowadzenie zmian w ewidencjach, rozpatrzone skargi i wnioski, dokumentacja obsługi posiedzeń ZPW, Komisji RPW, sesji RPW i inne w zależności od prowadzonych spraw) ze wskazaniem, czy przekroczone zostały terminy biegu spraw wynikające z przepisów prawnych.

2. Informacja na temat: uchylonych decyzji, wydanych postanowień w sprawie sprostowania z urzędu lub na żądanie strony błędów pisarskich i rachunkowych oraz innych oczywistych omyłek w wydanych decyzjach, zmian umów (aneksy do umów) wynikających z nieprawidłowych zapisów umów, uchylonych uchwał RP W i ZPW, (uznane za niezgodne z prawem przez organ nadzorczy).
3. Informacja o działaniach podjętych w związku z wystąpieniem nieprawidłowości wskazanych w pkt 2.
4. Informacja o sposobie realizacji zaleceń pokontrolnych, po kontrolach zewnętrznych i wewnętrznych, które wpłynęły w okresie sprawozdawczym oraz kontynuowanych z poprzedniego okresu.
5. Ogólna ocena jakości realizowanych zadań i usług świadczonych przez wydział.
6. Propozycje usprawnienia działania wydziału/samodzielnego stanowisk

**Załącznik nr 3 do Zasad planowania celów i zadań
do realizacji oraz sporządzania sprawozdań
dla Starostwa Powiatowego w Kępnie
i jednostek organizacyjnych Powiatu Kępińskiego**

Oświadczenie o stanie kontroli zarządczej
za rok
(rok, za który składane jest oświadczenie)

Jako osoba odpowiedzialna za zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej, tj. działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy, a w szczególności dla zapewnienia:

1. zgodności działalności z przepisami prawa i procedurami wewnętrznymi,
2. skuteczności i efektywności działania,
3. wiarygodności sprawozdań,
4. ochrony zasobów,
5. przestrzegania i promowania zasad etycznego postępowania,
6. efektywności i skuteczności przepływu informacji,
7. zarządzania ryzykiem,

oświadczam, że¹⁾ w kierowanej przeze mnie jednostce sektora finansów publicznych, tj.

.....
.....

(nazwa jednostki sektora finansów publicznych)

CZĘŚĆ A²⁾

w wystarczającym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.

CZĘŚĆ B³⁾

w ograniczonym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.

1) Zastrzeżenia dotyczą⁴⁾:

.....
.....
.....
.....
.....
.....
.....

2) Zostaną podjęte następujące działania w celu poprawy funkcjonowania kontroli zarządczej⁵⁾:

.....
.....
.....
.....
.....
.....
.....
.....
.....

Część C⁶⁾:



nie funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.

1) Zastrzeżenia dotyczą⁴⁾:

.....
.....
.....
.....
.....
.....

2) Zostaną podjęte następujące działania w celu poprawy funkcjonowania kontroli zarządczej⁵⁾:

.....
.....
.....
.....
.....
.....
.....
.....

CZĘŚĆ D⁷⁾:

W ubiegłym roku zostały podjęte następujące działania w celu poprawy funkcjonowania kontroli zarządczej:

.....
.....
.....
.....
.....

.....
.....
.....
.....

Część E

Niniejsze oświadczenie opiera się na mojej ocenie i informacjach dostępnych w czasie sporządzania niniejszego oświadczenia pochodzących z⁸⁾:

- monitoringu realizacji celów i zadań,
 - samooceny kontroli zarządczej przeprowadzonej z uwzględnieniem standardów kontroli zarządczej dla sektora finansów publicznych⁹⁾
 - systemu zarządzania ryzykiem,
 - kontroli wewnętrznych,
 - kontroli zewnętrznych,
 - innych
- informacji:..... źródła

.....
.....
.....

Jednocześnie oświadczam, że nie są mi znane inne fakty lub okoliczności, które mogłyby wpłynąć na treść niniejszego oświadczenia.

.....
(miejscość, data)

.....
(podpis kierownika jednostki)

**Załącznik nr 4 do zarządzenia
Nr 16/2023 Starosty Kępińskiego
z dnia 6 kwietnia 2023r.**

ZASADY DOKONYWANIA ANALIZY RYZYKA ORAZ USTALANIA SPOSOBÓW REAKCJI NA RYZYKO DLA STAROSTWA POWIATOWEGO W KĘPNIE I JEDNOSTEK ORGANIZACYJNYCH POWIATU KĘPIŃSKIEGO

Metodyka zarządzania ryzykiem w systemie kontroli zarządczej

1. Skróty i definicje stosowane w zarządzaniu ryzykiem

2. Identyfikacja ryzyka

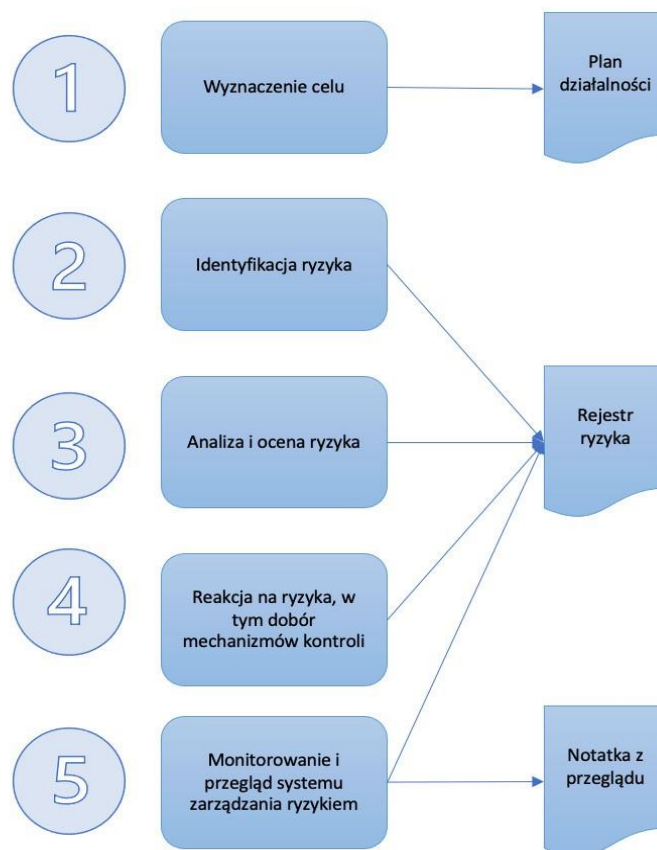
3. Ocena ryzyka

4. Dobór mechanizmów kontrolnych

5. Monitorowanie

Metodyka zawiera wytyczne i wskazówki do stosowania w zarządzaniu ryzykiem w ramach systemu kontroli zarządczej. **Celem metodyki jest zapewnienie adekwatnego, skutecznego i efektywnego systemu zarządzania ryzykiem.**

Proces zarządzania ryzykiem odbywa się zgodnie z przedstawionym schematem działania:



1. Skróty i definicje stosowane w zarządzaniu ryzykiem w systemie kontroli zarządczej

1) **Cel** – zaplanowane osiągnięcie stanu w przyszłości wraz z kluczowym rezultatem oraz zadaniami niezbędnymi do jego realizacji określony w planie działalności jednostki lub komórki organizacyjnej.

2) **Ryzyko** – niepewne zdarzenie lub zbiór niepewnych zdarzeń, które jeżeli wystąpią to wpłyną na osiągnięcie celów działalności lub zadań.

3) **Zdarzenie (materializacja ryzyka/nieprawidłowość)** – wydarzenie, incydent wewnętrzny lub zewnętrzny wpływający na osiągnięcie celu. Zdarzenia świadczą o wystąpieniu

czynnika ryzyka. Może dotyczyć ryzyka zidentyfikowanego i umieszczonego w Rejestrze ryzyka, jak i ryzyka, nie wskazanego w Rejestrze ryzyka.

4) **Zarządzanie ryzykiem** – jest procesem realizowanym przez kierownika jednostki, kierownika komórki organizacyjnej oraz wszystkich pracowników w celu świadomego i skutecznego radzenia sobie z niepewnością i związanymi z nią zagrożeniami i możliwościami, umożliwiającą ochronę wypracowanej wartości oraz zwiększenie zdolności do budowania wartości jednostki organizacyjnej.

5) **System Zarządzania Ryzykiem (SZR)** – jest to uporządkowany zbiór reguł i zasad, w sposób jednolity i stały stosowanych w odniesieniu do ryzyka prowadzonej działalności. SZR obejmuje następujące etapy:

a) identyfikację ryzyka i zdarzeń, które mogą wywrzeć wpływ na jednostkę lub komórkę organizacyjną,

b) ocenę ryzyka,

c) dobór mechanizmów kontroli oraz opracowanie i wdrożenie planów reakcji na ryzyko,

d) monitorowanie i raportowanie na temat skuteczności zarządzania ryzykiem.

6) **Czynnik ryzyka** – istniejący lub spodziewany stan faktyczny powodujący wystąpienie ryzyka w związku z realizacją celu lub zadania.

7) **Skutek ryzyka** – efekt materializacji ryzyka, która prowadzi do powstania nieprawidłowości.

8) **Prawdopodobieństwo ryzyka** – oczekiwana szansa materializacji (wystąpienia) danego ryzyka.

9) **Ocena ryzyka** – iloczyn prawdopodobieństwa i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiągnięcie przez zamierzonych celów.

10) **Mechanizm kontrolny** – polityki, procedury, regulacje wewnętrzne oraz czynności mające na celu wpływ na ograniczenie skutku lub prawdopodobieństwa materializacji ryzyka i jego wpływu na wyznaczony cel lub realizowane zadanie.

11) **Reakcja na ryzyko** – określony sposób reakcji na ryzyko wynikający z oceny ryzyka pod względem jego wpływu i prawdopodobieństwa oraz aktualnej oceny mechanizmów kontroli.

12) **Rejestr ryzyka** – udokumentowany zbiór zidentyfikowanych ryzyk.

13) **Strategia zarządzania ryzykiem** – kierunek, rodzaj pożądanych działań w zakresie zarządzania danym ryzykiem z dopuszczalnym poziomem akceptacji ryzyka. Strategie zarządzania ryzykiem mogą obejmować następujące rodzaje działań:

a) **Redukcja (ograniczenie) ryzyka** - podjęcie działań w kierunku ograniczenia prawdopodobieństwa lub skutku zdarzenia, lub obydwu jednocześnie.

b) **Transfer ryzyka** - ograniczanie prawdopodobieństwa i skutków ryzyka poprzez przekazanie całego lub części ryzyka innej stronie.

c) **Unikanie ryzyka** - odejście od działań, które wiążą się z ryzykiem,

d) **Akceptacja ryzyka** – świadomość istnienia ryzyka, przy jednoczesnym zapewnieniu minimalnego poziomu kontroli ryzyka z zachowaniem zasad należytej staranności działania w zakresie jego monitorowania.

14) **Właściciel ryzyka** – osoba, która ze względu na zajmowane stanowisko i przydział odpowiedzialności zarządza czynnikami ryzyka i ma wpływ na ograniczenie skutku lub prawdopodobieństwa ryzyka. Właścicielem ryzyka w zależności od okoliczności jest kierownik jednostki, kierownik komórki organizacyjnej lub osoba na samodzielnym stanowisku pracy.

15) **Plan działania** – czynności niezbędne do ograniczenia ryzyka poprzez ograniczenie skutku lub prawdopodobieństwa ocenionego ryzyka.

2. Identyfikacja ryzyka

2.1. Identyfikacja ryzyka jest procesem ciągłym i polega na ustaleniu możliwości wystąpienia określonych zdarzeń, które będą miały wpływ na realizację poszczególnych celów i zadań.

2.2. Kierownik jednostki organizacyjnej zarządza przeprowadzenie identyfikacji/aktualizacji ryzyka, nie rzadziej niż raz w roku, w terminie do 31 grudnia danego roku.

2.3. Kierownik jednostki może zarządzić częstsze przeprowadzanie identyfikacji ryzyka, o ile uzna to za konieczne z punktu widzenia realizacji celów i zadań.

2.4. Właściciel ryzyka dokonuje identyfikacji ryzyka w odniesieniu do celów i zadań określonych w planie działalności jednostki oraz komórki organizacyjnej.

2.5. Kierownik jednostki organizacyjnej może podjąć, o ile uzna to za stosowne powołanie stałego lub doraźnego zespołu do spraw zarządzania ryzykiem, któremu powierza zadania w zakresie identyfikacji i oceny ryzyka. Właściciel ryzyka jest zobowiązany do współpracy z zespołem do spraw zarządzania ryzykiem w zakresie, który dotyczy jego działalności oraz realizowanych celów i zadań.

2.6. Identyfikacja ryzyka jest przeprowadzana na podstawie:

- a) informacji i przewidywań pochodzących od pracowników;
- b) wcześniejszych doświadczeń i analiz;
- c) doświadczeń, wynikających z działalności innych podmiotów, które realizują cele i zadania w obszarze, w jakim działa jednostka lub komórka organizacyjna;
- d) wyników kontroli zewnętrznych, audytów wewnętrznych, przeglądów kierowniczych oraz innych form weryfikacji, kontroli i nadzoru.

2.7. Identyfikację ryzyka przeprowadza się każdorazowo w przypadku stwierdzenia zdarzenia (materializacji ryzyka/nieprawidłowości), wynikającego z wyników przeprowadzonych kontroli zewnętrznych, audytów wewnętrznych lub innych przeglądów sposobu realizacji celów i zadań.

2.8. Informacje o ryzykach gromadzone są w prowadzonym pisemnie oraz elektronicznie Rejestrze ryzyka stanowiącym załącznik nr 1 do niniejszych zasad.

2.9. Każdy pracownik jest odpowiedzialny za niezwłoczne zgłaszanie właścicielowi ryzyka informacji o nowym ryzyku, zidentyfikowanym w trakcie wykonywanych przez siebie obowiązków.

2.10. Pracownik, który zidentyfikował nowe ryzyko przekazuje właścicielowi ryzyka informacje odnośnie tego ryzyka oraz jego prawdopodobieństwa i skutków drogą służbową w formie pisemnej lub powszechnie stosowanej w jednostce formie..

2.11. Właściciel ryzyka dokonuje wstępnej analizy ryzyka, przeprowadzając ocenę prawdopodobieństwa i skutków tego ryzyka oraz wprowadza ryzyko do Rejestru ryzyka.

2.12. Ostateczną decyzję o zatwierdzeniu ryzyka podejmuje Kierownik jednostki lub osoba przez niego upoważniona.

2.13. Ryzyka w systemie kontroli zarządczej są identyfikowane z uwzględnieniem następujących rodzajów:

- a) **Ryzyko strategiczne**, oznacza zagrożenia dotyczące planowania i działalności w perspektywie długoterminowej związane z działalnością organizacji, jako całości;
- b) **Ryzyko organizacyjne**, oznacza zagrożenia dotyczące organizacji bieżącej realizacji zadań oraz procesów zarządczych;
- c) **Ryzyko nieetycznego zachowania**, oznacza zagrożenie dotyczące naruszania przez kierownictwo lub pracowników wartości, zasad etycznych organizacji oraz zasad współżycia społecznego;
- d) **Ryzyko nadużyć**, oznacza zagrożenie dotyczące wystąpienia umyślnego działania lub zaniechania, mającego na celu oszukanie (wprowadzenie w błąd) innych osób w celu uzyskania osobistej korzyści sprawcy, która powoduje stratę pokrzywdzonego;

- e) **Ryzyko kadrowe**, oznacza zagrożenia dotyczące dostępności do wykwalifikowanych i doświadczonych pracowników, jak również ograniczenia wsparcia ekspertów zewnętrznych;
- f) **Ryzyko finansowe i rachunkowe**, oznacza zagrożenia dotyczące ograniczenia lub utraty środków finansowania działalności oraz rejestrowania transakcji w systemach finansowo-księgowych z naruszeniem obowiązujących przepisów i standardów rachunkowości;
- g) **Ryzyko prawne**, oznacza zagrożenia dotyczące naruszenia przepisów prawa powszechnie obowiązującego lub regulacji wewnętrznych;
- h) **Ryzyko zawierania umów**, oznacza zagrożenia dotyczące nawiązywania stosunków gospodarczych z podmiotami zewnętrznymi;
- i) **Ryzyko techniczne**, oznacza zagrożenia dotyczące dostępności środków, sprzętu oraz wyposażenia technicznego, pozwalających na realizację celów;
- j) **Ryzyko technologii informatycznych**, oznacza zagrożenia dotyczące wykorzystywania w realizacji celów sieci, systemów i narzędzi informatycznych;
- k) **Ryzyko bezpieczeństwa informacji**, oznacza zagrożenia dotyczące nawiązywania stosunków gospodarczych z podmiotami zewnętrznymi;
- l) **Ryzyko naruszenia danych osobowych**, oznacza zagrożenia dotyczące gromadzenia i przetwarzania danych osobowych z naruszeniem przepisów prawa;
- m) **Ryzyko bezpieczeństwa informacji**: zagrożenia dotyczące ujawniania istotnych informacji osobom nieupoważnionym;
- n) **Inne ryzyko**, oznacza rodzaj ryzyka wcześniej nie sklasyfikowany.

2.14. Przy identyfikacji czynników ryzyka w ramach poszczególnych rodzajów ryzyka właściciel ryzyka korzysta z listy czynników ryzyka, określonych w pkt. 6.

2.15. Właściciel ryzyka może wystąpić do Kierownika jednostki o uzupełnienia listy ryzyk jeżeli nie zawiera ono czynnika ryzyka, który został zidentyfikowany w trakcie identyfikacji.

2.16. Szczegółową metodyką zarządzania ryzykiem bezpieczeństwa informacji określają procedury systemu zarządzania bezpieczeństwem informacji.

2.17. Szczegółową metodykę zarządzania ryzykiem danych osobowych określają procedury ochrony danych osobowych.

3. Ocena ryzyka

3.1. Ocena ryzyka jest przeprowadzana w terminach i na zasadach określonych w pkt. 2.2. i ma na celu określenie prawdopodobieństwa wystąpienia oraz możliwych skutków ryzyka, które mają wpływ na osiągnięcie celów i zadań.

3.2. Ocenę ryzyka przeprowadza właściciel ryzyka. Jeżeli Kierownik jednostki podjął decyzję o powołaniu zespołu do spraw zarządzania ryzykiem oceny ryzyka dokonuje zespół we współpracy z właścicielem ryzyka każdego z obszarów działalności jednostki organizacyjnej.

3.3. Wyniki oceny ryzyka są zatwierdzane przez Kierownika jednostka lub osobę przez niego upoważnioną. Ocena ryzyka i jego aktualizacja dokumentowana jest w rejestrze ryzyka.

3.4. Właściciel ryzyka, a w przypadku powołania, zespół do spraw zarządzania ryzykiem wspólnie z właścicielem ryzyka dokonuje oceny:

- a) ryzyka, które wpłynie na osiągnięcie i realizację zadań, określonych w planie działalności oraz wynikających z działalności statutowej jednostki organizacyjnej;
- b) adekwatności, skuteczności i efektywności istniejących mechanizmów kontrolnych.

3.5. Dokonując oceny ryzyka bierze się pod uwagę:

- a) ocenę adekwatność, skuteczność i efektywność istniejącego mechanizmu kontrolnego,
- b) skutki wpływu ryzyka na cele działalności i zadania, określone w planie działalności oraz wynikających z działalności statutowej jednostki organizacyjnej;
- c) prawdopodobieństwo wystąpienia ryzyka.

3.6. Oceniając **adekwatność, efektywność i skuteczność** aktualnie stosowanych mechanizmów kontrolnych analizuje się m.in.:

- a) czy istnieją określone mechanizmy kontrolne (procedury kontroli ryzyka oraz inne działania zmierzające do ograniczenia skutków i prawdopodobieństwa ryzyka);
- b) czy mechanizmy kontrolne są dostosowane do charakteru ryzyka i pozwalają na skuteczne zarządzanie ryzykiem;
- c) czy istniejące mechanizmy kontrolne są realizowane prawidłowo, tj. czy doszło do nieprawidłowości w obszarze działalności właściciela ryzyka;
- d) czy istnieją możliwości poprawy skuteczności zarządzania danym ryzykiem,
- e) wyniki kontroli zewnętrznych, audytu wewnętrznego lub innych przeglądów i weryfikacji.

3.7. Przy ocenie mechanizmu kontrolnego stosuje się następującą skalę oceny:

- a) **nieskuteczny (1 pkt)**, co oznacza brak mechanizmu kontrolnego lub nie jest stosowany w praktyce;
- b) **mało skuteczny (2 pkt)**, co oznacza, że mechanizm kontrolny został wdrożony, lecz w działalności występują istotne nieprawidłowości bezpośrednio zagrażające osiągnięciu celu lub nie przeprowadzono weryfikacji skuteczności mechanizmu kontroli (np. w formie przeglądu kierowniczego);
- c) **średnio skuteczny (3 pkt)**, co oznacza, że mechanizm kontrolny został wdrożony, lecz w działalności występują nieprawidłowości pośrednio zagrażające osiągnięciu celu lub nie przeprowadzono udokumentowanej weryfikacji skuteczności mechanizmu kontroli (np. w formie kontroli zewnętrznej, audytu wewnętrznego lub innej udokumentowanej weryfikacji);
- d) **skuteczny (4 pkt)**, co oznacza, że mechanizm kontrolny został wdrożony i zweryfikowano jego skuteczność, lecz w działalności występują nieistotne uchybienia,
- e) **bardzo skuteczny (5 pkt)**, co oznacza, że mechanizm został wdrożony, a w działalności nie występują nawet uchybienia.

3.8. Oceniając **wpływ ryzyka**, uwzględnia się możliwość wystąpienia skutków ryzyka, które mogą obejmować m.in.:

- a) naruszenie przepisów prawa powszechnie obowiązującego;
- b) naruszenie regulacji wewnętrznych;
- c) nieosiągnięcie lub opóźnienie realizacji celu;
- d) niezadowalającą jakość zrealizowanego celu;
- e) koszty realizacji celu zbyt wysokie w stosunku do uzyskanych rezultatów;
- f) ujawnienie na zewnątrz informacji podlegających ochronie;
- g) wykorzystanie danych lub informacji niezgodnie z przeznaczeniem;
- h) stratę finansową nieznacznych rozmiarów;
- i) stratę finansową znacznych rozmiarów;
- j) spadek przychodów/dochodów;
- k) wzrost kosztów/wydatków realizacji zadania;
- l) utratę lub zniszczenie aktywów/mienia;
- m) wykorzystanie aktywów/mienia niezgodnie z przeznaczeniem;
- n) zagrożenie ciągłości działania;
- o) niewiarygodne lub nierzetelne sprawozdanie;
- p) nieskuteczną i/lub nieefektywną komunikację między pracownikami;
- q) nieskuteczną i/lub nieefektywną komunikację między komórkami organizacyjnymi;
- r) negatywne informacje w mediach lokalnych;
- s) negatywne informacje w mediach krajowych;
- t) brak satysfakcji klienta zewnętrznego (interesariusza);
- u) niską skuteczność i nieefektywność zarządzania ryzykiem.

3.9. Przy ocenie skutku ryzyka stosuje się następującą skalę oceny:

- a) **niewielki (1 pkt)**, co oznacza brak lub niezauważalny wpływ ryzyka na działalność;

- b) **ograniczony** (2 pkt), co oznacza wpływ ryzyka (prawny, finansowy, organizacyjny, wizerunkowy) ograniczony do działalności danej komórki organizacyjnej;
- c) **średni** (3 pkt), co oznacza wpływ ryzyka (prawny, finansowy, organizacyjny, wizerunkowy) na działalność innych komórek organizacyjnych lub całej jednostki;
- d) **znaczący** (4 pkt), co oznacza wpływ ryzyka na podmioty zewnętrzne (klientów, petentów, wykonawców, dostawców, innych interesariuszy);
- e) **bardzo duży** (5 pkt), co oznacza, że materializacja ryzyka/nieprawidłowość zagrozi ciągłości działania jednostki;
- f) **jeżeli skuteczność mechanizmu kontrolnego została oceniona jako mniej niż średnio skuteczna skutek ryzyka może być oceniony jako średni, znaczący lub bardzo duży.**

3.10. Przy ocenie prawdopodobieństwa ryzyka stosuje się następującą skalę oceny:

- a) **wątpliwe (1 pkt)**, co oznacza brak lub mniej niż szacunkowo 10% szansy na materializację ryzyka (wypowiedź oceniającego: zdecydowanie nie zgadzam się, że ryzyko istnieje);
- b) **mało prawdopodobne (2 pkt)**, co oznacza, że istnieje szansa w szacunkowych granicach od 11 do 40% materializacji ryzyka (wypowiedź oceniającego: raczej nie zgadzam się, że ryzyko istnieje);
- c) **możliwe (3 pkt)** - jest możliwe, że w szacunkowych granicach od 41 do 60% wystąpi materializacja ryzyka (wypowiedź oceniającego: trudno powiedzieć, czy ryzyko istnieje);
- d) **realne (4 pkt)** - szansa na wystąpienie ryzyka szacunkowo wynosi od 61 do 80% (wypowiedź oceniającego: zgadzam się, że ryzyko istnieje);
- e) **prawie pewne (5 pkt)** - szansa na wystąpienie ryzyka szacunkowo przekracza 90% (wypowiedź oceniającego: zdecydowanie zgadzam się, że ryzyko istnieje);
- f) **jeżeli skuteczność mechanizmu kontrolnego została oceniona jako mniej niż średnio skuteczna prawdopodobieństwo ryzyka może być ocenione jako możliwe, realne lub prawie pewne.**

3.11. Po dokonaniu oceny skutków i prawdopodobieństwa ryzyka właściciel ryzyka w stosunku do każdego ryzyka określa bliskość ryzyka, czyli czas w jakim działając z zachowaniem należytej ostrożności spodziewa się materializacji ryzyka lub czas w jakim planowana jest kolejna ocena ryzyka.

3.12. Kolejna ocena ryzyka uzależniona jest od wagi stwierdzonego zagrożenia i następuje w terminie określonym przez właściciela i może być przeprowadzona w ciągu: a) miesiąca;

- b) trzech miesięcy;
- c) sześciu miesięcy;
- d) dwunastu miesięcy.

4. Dobór mechanizmów kontrolnych

4.1. Mechanizmy kontrolne mają na celu ograniczenie skutków lub prawdopodobieństwa wystąpienia ryzyka i jego wpływu na założone cele oraz realizowane zadania.

4.2. Właściciel ryzyka jest odpowiedzialny za zaprojektowanie i wdrożenie mechanizmu kontrolnego ryzyka na podstawie przeprowadzonej oceny ryzyka z zachowaniem zasad należytej staranności działania oraz profesjonalnego osądu, związanego z doświadczeniem w obszarze, za który odpowiada.

4.3. W przypadku powołania zespołu do spraw zarządzania ryzykiem właściciel ryzyka uzgadnia mechanizm kontrolny z zespołem.

4.4. Kierownik jednostki lub upoważniony przez niego pracownik zatwierdza mechanizm kontroli zaproponowany przez właściciela ryzyka.

4.5. Mechanizm kontrolny projektuje się na uwzględniając strategię działania z ryzykiem, na przyjętą na podstawie wyników oceny ryzyka:

Ocena ryzyka: <ul style="list-style-type: none"> ▪ Niskie (1-4 pkt); □ Średnie (5-9 pkt); ▪ Wysokie (10-25 pkt). 			Skutek ryzyka				
			Niewielki	Ograniczony	Średnie	Znaczący	Bardzo duży
			1	2	3	4	5
Prawdopodobieństwo ryzyka	Wątpliwe	1	1	2	3	4	5
	Mało prawdopodobne	2	2	4	6	8	10
	Możliwe	3	3	6	9	12	15
	Realne	4	4	8	12	16	20
	Prawie pewne	5	5	10	15	20	25

Ocena	Zalecana strategia działania
25	Strategia: Unikanie/Transfer/Redukcja ryzyka Działania: <ul style="list-style-type: none"> ▪ Obniżenie prawdopodobieństwa lub skutku wystąpienia ryzyka poprzez wzmocnienie istniejącego mechanizmu kontrolnego oraz obligatoryjne wprowadzenie dodatkowego. ▪ Przegląd raz na kwartał. ▪ Informacja o wynikach przeglądu jest przekazywana do Kierownika jednostki
20	
16	
15	
12	
10	
9	Strategia: Transfer/Redukcja ryzyka Działania: <ul style="list-style-type: none"> □ Bieżące monitorowanie skuteczności i efektywności dotychczas stosowanego mechanizmu kontrolnego lub fakultatywne wprowadzenie dodatkowego
8	
6	
5	mechanizmu kontrolnego. <ul style="list-style-type: none"> ▪ Przegląd na pół roku.

	<ul style="list-style-type: none"> ▪ Informacja o wynikach przeglądu jest przekazywana do Kierownika jednostki.
4	Strategia: Akceptacja/Monitorowanie
3	Działanie: <ul style="list-style-type: none"> ▪ Wstępna akceptacja ryzyka i monitorowanie skuteczności i efektywności mechanizmu kontrolnego.
2	
1	<ul style="list-style-type: none"> ▪ Przegląd raz w roku.

4.6. Projektując mechanizm kontrolny właściciel bierze pod uwagę:

- a) rodzaj wyznaczonego celu i zadań przyjętych do jego osiągnięcia oraz skutki finansowe, prawne, organizacyjne i wizerunkowe;
- b) możliwość podjęcia działań polegających na:
 - zapobieganiu wystąpieniu ryzyka (mechanizmy prewencyjne)
 - ograniczeniu skutków ryzyka (mechanizmy wykrywające i korygujące);
- e) ewentualne koszty wdrożenia mechanizmu kontrolnego.

4.7. Katalog mechanizmów kontrolnych może obejmować m.in.

- a) planowanie działalności/harmonogram pracy;
- b) analizę ryzyka;
- c) opracowanie lub uszczegółowienie polityki i procedur wewnętrznych;
- d) przydział zadań w strukturze organizacyjnej;
- e) podział obowiązków pomiędzy różne osoby;
- f) rotację na stanowisku;
- g) nadzór przełożonego;
- h) nadzór prawny;
- i) bieżący monitoring;
- j) udzielenie upoważnienia/wprowadzenie limitów do podejmowania decyzji finansowych i gospodarczych;
- k) weryfikację wyników pracy przez inną osobę;
- l) zatwierdzenie wyników pracy przez inną osobę;
- m) sprawozdawczość z realizacji zadań/raportowanie
- n) rejestrację danych w systemie IT lub dedykowanej aplikacji;
- o) weryfikację danych w systemie IT lub dedykowanej aplikacji;
- p) automatyczną kontrolę wprowadzania danych w systemie IT;
- q) fizyczną kontrolę dostępu;
- r) prowadzenie rejestru/ewidencji;
- s) weryfikację stanu faktycznego/inwentaryzację;
- t) weryfikację kontrahenta/dostawy/wykonawcy;
- u) zawarcie postanowień w umowach/klauzul umownych;
- v) uzgodnienia danych w różnych źródłach;
- w) instruktaż stanowiskowy;
- x) szkolenie pracowników;
- y) spotkanie zespołu/spotkania z pracownikami;
- z) opracowanie scenariusza działania; aa) przegląd kierowniczy; bb) dofinansowanie działalności ze źródeł zewnętrznych; cc) przeprowadzenie postępowania

sprawdzającego/wyjaśniającego; dd) przeprowadzenie audytu wewnętrznego ee) doradztwo zewnętrzne/zatrudnienie eksperta w danej dziedzinie

5. Monitorowanie i przegląd systemu zarządzania ryzykiem

5.1. Właściciel ryzyka jest odpowiedzialny za bieżące monitorowanie aktualności danych ujętych w Rejestrze ryzyka. Bieżące monitorowanie polega w szczególności na:

- a) zapewnieniu zgłaszania przez pracowników właścicielowi ryzyka nowych właścicielowi ryzyka,
- b) zmianie oceny ryzyka już zidentyfikowanego, o ile wystąpią okoliczności uzasadniające takie działanie;
- c) ponownej ocenie ryzyka w terminie uwzględniającym założoną bliskość ryzyka;
- d) zgłaszanie Kierownikowi jednostki potrzeb dotyczących usprawniania systemu zarządzania ryzykiem.

5.2. Częstotliwość działań właściciela ryzyka uwzględnia terminy identyfikacji ryzyka, o których mowa w pkt. 2.2. oraz strategii działania, określonej w pkt. 4.3.

5.3. Kierownik jednostki nie rzadziej niż raz w roku w terminie do 31 stycznia roku następnego dokonuje przeglądu całego systemu zarządzania ryzykiem oraz zapewnia jego dostosowanie do wyznaczonych celów i zadań.

5.4. Wyniki przeglądu systemu zarządzania ryzykiem dokumentuje się w formie notatki służbowej.

5.5. Przegląd systemu zarządzania ryzykiem obejmuje w szczególności:

- a) analizę przydzielonych ról, zadań i odpowiedzialności;
- b) analizę adekwatności, skuteczności i efektywności podejmowanych działań;
- c) sformułowanie zaleceń usprawniających funkcjonowanie systemu zarządzania ryzykiem.

5.6. Oceniając adekwatność, skuteczność i efektywność systemu zarządzania ryzykiem kierownik jednostki bierze w pod uwagę w szczególności kluczowe rezultaty (mierniki):

- a) liczbę pracowników przeszkolonych w zakresie zarządzania ryzykiem od czasu poprzedniego przeglądu;
- b) liczbę nowych ryzyk zidentyfikowanych od czasu poprzedniego przeglądu;
- c) liczbę ryzyk, w przypadku których ograniczono skutek oraz prawdopodobieństwo wystąpienia od czasu poprzedniego przeglądu;
- d) liczbę ryzyk, w przypadku których od czasu poprzedniego przeglądu dokonano udokumentowanej weryfikacji skuteczności mechanizmów kontroli;
- e) liczbę stwierdzonych od czasu poprzedniego przeglądu materializacji ryzyka/nieprawidłowości.

5.7. W zakresie monitorowania Kierownik jednostki oraz właściciel ryzyka współpracują z audytem wewnętrznym, który może wskazać szczegółową metodę oraz wymogi przeprowadzenia przeglądu systemu zarządzania ryzykiem.

Lista czynników ryzyka

Lp.	Czynniki ryzyka strategicznego
1.	Brak lub niejasna misja i wizja, w tym niejasna komunikacja ogółowi pracowników
2.	Brak lub nieadekwatne do rzeczywistości plany długoterminowe
3.	Brak lub nieskuteczne zasady zarządzania ryzykiem strategicznym

4.	Brak możliwości prowadzenia działalności w obecnej lokalizacji
6.	Brak planów ochrony krytycznej infrastruktury lub planów ciągłości działania
7.	Brak planów ciągłości działania lub odstąpienie od ich aktualizacji
8.	Brak zastępowalności na kluczowych stanowiskach
9.	Brak zasad zarządzania zagrożeniem terroryzmem
10.	Brak lub niejasne zasady zarządzania wizerunkiem organizacji oraz kontaktowania się z mediami i opinią publiczną
11.	Brak lub niezetelna weryfikacja zewnętrznych pomiotów współpracujących
12.	Wysoka wrażliwość polityczna prowadzonej działalności
13.	Brak zasad zarządzania zmianami

Lp.	Czynniki ryzyka organizacyjnego
1.	Brak lub niejasno przypisana odpowiedzialność za realizację celów i zadań
2.	Brak lub nieadekwatne do rzeczywistości planowanie realizacji zadań
3.	Brak lub nieskuteczne zasady zarządzania ryzykiem operacyjnym
4.	Niejasno określone standardy pracy oraz realizowanych zadań
5.	Niejasne priorytety realizowanych zadań
6.	Nieefektywna organizacja realizacji zadań, w tym nierównomierne obciążenie pracowników zadaniami
7.	Brak lub nieefektywne monitorowanie realizacji zadań, w tym niezapewnienie niezależnego audytu lub kontroli
8.	Brak zastępowalności pracownika w czasie jego nieobecności
9.	Brak zasad i procedur zapewnienia ciągłości działania operacyjnego

Lp.	Czynniki ryzyka nieetycznego zachowania
1.	Nierówne traktowanie pracownika w związku z wykonywanymi zadaniami niezależnie od powodu
2.	Zachęcanie do nierównego traktowania pracownika w związku z wykonywaniem zadaniami niezależnie od powodu
3.	Molestowanie pracownika w związku z wykonywanymi zadaniami, polegające na naruszeniu godności, poniżeniu lub upokorzeniu

5.	Naruszenie zasad współżycia społecznego w miejscu pracy oraz w związku z wykonywaną pracą
4.	Molestowanie seksualne, polegające na nieakceptowanym przez pracownika zachowaniu o charakterze seksualnym, mający charakter fizyczny, werbalny lub poza werbalny

Lp.	Czynniki ryzyka nadużyć
1.	Korupcja: Konflikt interesów przy realizacji zadań, który wpływa na podejmowane decyzje
2.	Korupcja: Przekupstwo, polegające na oferowaniu lub przyjmowaniu łapówek
3.	Korupcja: Przyjmowanie lub oferowanie dowodów wdzięczności, celem uzyskania osobistych korzyści
4.	Korupcja: Wymuszenie korzyści w celu ujawniania poufnych informacji lub podjęcia decyzji skutkującej korzyścią dla podmiotu lub osoby spoza organizacji
5.	Kradzież gotówki w kasie
6.	Kradzież płatności wynikających z wystawionych faktur zanim zostaną ujęte w księgach i rejestrach organizacji
7.	Niezasadne wydatki wynikające z faktur za fikcyjne towary lub usługi, zawyżone faktury lub faktury za wydatki osobiste
8.	Falszowanie dokumentacji (np. faktur, list płac, wniosków kredytowych, wniosków o dofinansowanie, dokumentacji rozliczeniowej)
9.	Nieuzasadnione zwroty kosztów związane z fikcyjnymi lub zawyżonymi wydatkami służbowymi
10.	Przechwytywanie lub falszowanie płatności dokonywanych drogą elektroniczną
11.	Manipulowanie rejestrami wpłat lub wypłat w celu ukrycia nieuczciwego pobrania gotówki
12.	Niewłaściwe wykorzystanie, w celach prywatnych, zasobów niepieniężnych pozostawionych pracownikowi do jego dyspozycji
13.	Kradzież zapasów lub innych aktywów niepieniężnych
14.	Zawyżanie lub zaniżanie faktycznych dochodów w celu zniekształcenia danych finansowych
15.	Rejestrowanie operacji w nieodpowiednich okresach w celu zniekształcenia danych finansowych
16.	Zaniżanie lub zawyżanie zobowiązań lub wydatków celem zniekształcenia danych finansowych
17.	Manipulowanie wyceną aktywów
18.	Manipulowanie informacjami wykazywanymi w ewidencji finansowo-księgowej oraz w sprawozdaniach

Lp.	Czynniki ryzyka kadrowego
1.	Nieobsadzone stanowiska pracy
2.	Trudności w pozyskaniu pracownika w procesie rekrutacji
3.	Odejście kluczowych pracowników/pracownika z pracy
4.	Brak zastępowalności na kluczowych stanowiskach
5.	Brak planów sukcesji na kluczowych stanowiskach pracy
6.	Niewystarczające umiejętności lub doświadczenie pracowników
7.	Niezadowolenie pracowników z warunków zatrudnienia
8.	Brak lub niewystarczająca liczba szkoleń pracowników
9.	Konflikty w relacjach między pracownikami lub między pracownikami a przełożonym
10.	Skargi na pracowników od podmiotów zewnętrznych

Lp.	Czynniki ryzyka finansowego i rachunkowego
1.	Zbyt niski budżet w stosunku do potrzeb i realizowanych zadań
2.	Utrata lub odczuwalne ograniczenie istotnego źródła finansowania działalności
3.	Zwrot środków z tytułu nieprawidłowości w rozliczaniu wsparcia finansowego
4.	Błędy w opisie transakcji na dokumentach księgowych
5.	Brak lub nieskuteczna weryfikacja lub autoryzacja dokumentacji księgowej
7.	Błędy w rejestrowaniu transakcji w systemie finansowo-księgowym
8.	Zaciąganie zobowiązań bez upoważnienia lub z przekroczeniem zakresu upoważnienia
9.	Naruszenie dyscypliny finansów publicznych
10.	Brak weryfikacji warunków finansowych w zawieranych umowach
11.	Wzrost wydatków lub kosztów prowadzonej działalności

Lp.	Czynniki ryzyka prawnego
------------	---------------------------------

1.	Brak lub ograniczony dostęp do informacji o zmieniających się przepisach prawa
2.	Duża liczba niejasnych przepisów prawa, wymagających dodatkowej interpretacji
3.	Brak lub ograniczony dostęp do usług lub wsparcia prawniczego
4.	Brak lub niejasne regulacje wewnętrzne (wymagające dodatkowych interpretacji)
5.	Nadmierna liczba regulacji wewnętrznych powodująca nieefektywne działanie
6.	Rosnąca liczba naruszeń regulacji wewnętrznych
7.	Działanie bez lub z naruszeniem podstawy prawnej
8.	Rosnąca liczba naruszeń przepisów prawa
9.	Rosnąca liczba spraw lub pozwów sądowych
10.	Rosnąca liczba przegranych spraw sądowych

Lp.	Czynniki ryzyka zawierania umów
1.	Brak uzasadnienia zawarcia umowy z punktu widzenia realizacji celów i zadań
2.	Brak lub niewystarczająca weryfikacja kontrahenta (wykonawcy umowy)
3.	Brak lub niewystarczające zabezpieczenie środków finansowych na realizację umowy
4.	Brak lub niewystarczające zabezpieczenie interesów prawnych organizacji w zawartej umowie
5.	Brak spełnienia w umowie wymogów wynikających z przepisów obowiązującego prawa lub wymagań regulatora
6.	Brak lub niewystarczający nadzór nad realizacją umowy

Lp.	Czynnika ryzyka technicznego
1.	Brak lub niewystarczające informacje na temat stanu technicznego obiektów infrastruktury lub mienia
2.	Brak lub nieregularne przeglądy stanu technicznego obiektów lub mienia
3.	Brak lub niewystarczające zabezpieczenie fizyczne obiektów lub mienia przed zdarzeniami losowymi lub awariami
4.	Brak lub nieaktualna inwentaryzacja stanu i ilości obiektów infrastruktury lub mienia
5.	Brak lub niewystarczające zabezpieczenie dostępu do obiektów lub mienia

7.	Brak przypisania jednoznacznej własności mienia powierzonego pracownikom do wykorzystania dla celów służbowych
8.	Brak określenia lub skutecznego nadzorowania zasad korzystania przez pracowników z aktywów i mienia organizacji
9.	Brak regularnych remontów lub konserwacji
10.	Brak zasad zwrotu i rozliczania mienia powierzonego pracownikom
11.	Brak lub niejasne zasady zapewnienia bezpieczeństwa pracownikom lub innym osobom, w związku z korzystaniem z aktywów i mienia organizacji

Lp.	Czynniki ryzyka technologii informatycznych
1.	Brak lub niewystarczające informacje na temat ilości zasobów sieci i sprzętu teleinformatycznego
2.	Brak lub nieregularne przeglądy stanu technicznego sieci i sprzętu teleinformatycznego
3.	Brak lub niewystarczające zabezpieczenie fizyczne sieci i sprzętu teleinformatycznego przed zdarzeniami losowymi lub awariami
4.	Brak lub nieaktualna inwentaryzacja stanu sieci i sprzętu teleinformatycznego
5.	Brak lub niejasne zasady dostępu do sieci urządzeń teleinformatycznych
6.	Brak lub niewystarczające zabezpieczenie dostępu do sieci i sprzętu teleinformatycznego
7.	Brak lub nieskuteczna ochrona antywirusowa lub brak ochrony przed złośliwym oprogramowaniem
8.	Brak lub nieregularne tworzenie kopii zapasowych informacji przetwarzanych w systemach teleinformatycznych
9.	Brak lub niejasne zasady używania przez pracowników nośników informatycznych
10.	Brak lub niejasne zasady ochrony dokumentacji systemów teleinformatycznych

Lp.	Czynniki ryzyka bezpieczeństwa informacji
1.	Brak lub niejasne zasady/polityki zarządzania bezpieczeństwem informacji
2.	Brak lub nieregularne przeglądy zasad/polityki zarządzania bezpieczeństwem informacji
3.	Brak lub niejasno przypisany zakres odpowiedzialność w zakresie bezpieczeństwa informacji
4.	Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników
5.	Brak lub niejasno określone zasady zachowania poufności przetwarzanych informacji przez podmioty zewnętrzne, np. w związku z realizowanymi umowami
6.	Brak lub niejasno określone zasady obiegu dokumentacji wewnątrz organizacji

7.	Brak lub niejasno określone zasady kontaktowania się pracowników z podmiotami zewnętrznymi, w tym korzystania przez pracowników z mediów społecznościowych w ramach realizowanych zadań
8.	Brak zabezpieczenia/inwentaryzacji miejsca przechowywania i nośników informacji
9.	Brak lub niejasne zasady udzielania informacji podmiotom zewnętrznym
10.	Brak lub nieregularne archiwizowanie informacji
11.	Brak lub niejasne zasady dostępu użytkowników do sieci teleinformatycznej, w tym rejestracji, udzielania przywilejów, zarządzania hasłami, oraz odbioru praw
12.	Brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych
13.	Brak lub niewłaściwa ochrona przed nieuprawnionym dostępem do informacji w aplikacjach, w tym luki w systemach
14.	Brak lub niejasne, w tym nieaktualne zasady pracy przy przetwarzaniu mobilnym i na odległość
15.	Brak lub niewłaściwa ochrona przed dokonywaniem nieuprawnionych zmian informacji w systemach i/lub aplikacjach
16.	Brak lub niewłaściwa ochrona bezpieczeństwa plików systemowych, w tym kodów źródłowych
17.	Brak lub niejasne zasady zarządzania incydentami bezpieczeństwa
18.	Brak działania lub działanie z opóźnieniem w sytuacji wystąpienia incydentów bezpieczeństwa teleinformatycznego
19.	Brak lub niewystarczające zapewnienie wsparcia teleinformatycznego w zawieranych umowach serwisowych
20.	Brak zapewnienia ciągłości działania systemów teleinformatycznych

Lp.	Czynniki ryzyka naruszenia danych osobowych
1.	Brak lub nieaktualna polityka/procedury przetwarzania danych osobowych
2.	Niepełny zakres regulacji zabezpieczających przetwarzanie danych osobowych
3.	Brak lub nieaktualne procedury postępowania w sytuacji naruszenia ochrony danych osobowych
4.	Wadliwe powołanie inspektora ochrony danych osobowych
5.	Brak lub niewystarczające kompetencje inspektora ochrony danych osobowych
6.	Naruszenie niezależności inspektora ochrony danych osobowych
7.	Brak lub niewystarczające zasoby do realizacji zadań inspektora ochrony danych osobowych
8.	Przetwarzanie danych w sytuacji braku lub niejasno wyrażonej zgody na przetwarzanie danych osobowych

9.	Brak lub niewystarczający nadzór nad umowami przetwarzania danymi osobowymi
10.	Brak lub niewystarczająca uzasadniona podstawa przetwarzania danych osobowych
11.	Brak lub niejasne cele przetwarzania danych osobowych
12.	Brak lub niska jakość procesu oceny przetwarzania danych osobowych
13.	Brak lub niekompletne rejestrowanie czynności przetwarzania danych osobowych
14.	Brak lub niewystarczające i nieadekwatne zarządzanie ryzykiem przetwarzania danych osobowych
15.	Brak lub niewystarczająca i nieadekwatne zabezpieczenie danych osobowych chronionych domyślnie lub na etapie projektowania
16.	Brak, niepełna lub nierzetelna ocena zakresu i skutków przetwarzania danych osobowych
17.	Brak lub nierzetelne prowadzenie rejestru naruszeń ochrony danych osobowych
18.	Zaniechanie zawiadamiania o naruszeniu danych osobowych uprawnionych organów zewnętrznych

**ZASADY DOKONYWANIA SAMOOCENY SYSTEMU KONTROLI ZARZĄDCZEJ ORAZ
UDZIELANIA INFORMACJI O STANIE KONTROLI ZARZĄDCZEJ DLA STAROSTWA
POWIATOWEGO W KĘPNIE I JEDNOSTEK ORGANIZACYJNYCH POWIATU KĘPIŃSKIEGO**

§ 1. Zasady dokonywania samooceny systemu kontroli zarządczej oraz udzielania informacji o stanie kontroli zarządczej ustalone niniejszym dokumentem obowiązują w Starostwie Powiatowym w Kępnie.

§ 2. 1. Ustalam obowiązek dokonywania samooceny systemu kontroli zarządczej w Starostwie Powiatowym, poprzez wypełnienie kwestionariusza samooceny **kontroli zarządczej - kierownicy komórek organizacyjnych** stanowiącego załącznik Nr 1 do niniejszych Zasad.

2. Ustalam obowiązek dokonywania samooceny systemu kontroli zarządczej w Starostwie Powiatowym w Kępnie, poprzez wypełnienie Kwestionariusza Samooceny **kontroli zarządczej - pracownik jednostki** , stanowiącego załącznik Nr 2 do niniejszych Zasad.

3. Ustalam termin przedłożenia wypełnionych kwestionariuszy, o których mowa w ust. 1 i 2 do 20 lutego za miniony rok.

**Załącznik Nr 1 do zasad samooceny systemu
kontroli zarządczej w Starostwie Powiatowym**

Kwestionariusz samooceny kontroli zarządczej - kierownicy komórek organizacyjnych

Lp.	PYTANIE	TAK	Odpowiedź TAK Dowody	NIE	Odpowiedź NIE- przyczyny	Trudn o oceni ć	Odpowiedź trudno to przyczyny ocenić-	Uwagi (propozycje)
1	Czy pracownicy są informowani o zasadach etycznego postępowania?							
2	Czy Pani/Pan wie jak należy się zachować, w przypadku gdy będzie Pani/Pan świadkiem poważnych naruszeń zasad etycznych obowiązujących w [jednostce]?							
3	Czy bierze Pan/Pani udział w szkoleniach w wystarczającym stopniu, aby skutecznie realizować powierzone zadania?							
4	Czy w Pani/Pana komórce organizacyjnej zostały pisemnie ustalone wymagania w zakresie wiedzy, umiejętności i doświadczenia konieczne do							

	wykonywania zadań na poszczególnych stanowiskach pracy (np. zakresy obowiązków, opisy stanowisk pracy)?							
5	Czy dokonuje Pani/Pan okresowej oceny pracy pracowników z Pani/Pana komórki organizacyjnej?							
6	Czy pracownicy zostali zapoznani z kryteriami, za pomocą których dokonuje Pani/Pan oceny wykonywania przez nich zadań? - należy odpowiedzieć tylko w przypadku, gdy odpowiedź na pytanie nr 5 brzmi TAK							
7	Czy pracownicy w Pani/Pana komórce organizacyjnej mają zapewniony w wystarczającym stopniu dostęp do szkoleń niezbędnych na zajmowanych przez nich stanowiskach pracy?							
8	Czy pracownicy w Pani/Pana komórce organizacyjnej posiadają							

	wiedzę i umiejętności konieczne do skutecznego realizowania przez nich zadań?							
9	Czy istniejące w [jednostce] procedury zatrudniania prowadzą do zatrudniania osób, które posiadają pożądane na danym stanowisku pracy wiedzę i umiejętności?							
10	Czy struktura organizacyjna Pani/Pana komórki organizacyjnej jest dostosowana do aktualnych jej celów i zadań?							
11	Czy struktura organizacyjna Pani/Pana komórki organizacyjnej jest okresowo analizowana i w miarę potrzeb aktualizowana?							
12	Czy w Pani/Pana komórce organizacyjnej zatrudniona jest odpowiednia liczba pracowników, w tym osób zarządzających, w odniesieniu do celów i zadań komórki?							

13	Czy przekazanie zadań i obowiązków pracownikom w Pani/Pana komórce organizacyjnej następuje zawsze w drodze pisemnej?							
14	Czy uprawnienia do podejmowania decyzji, zwłaszcza tych o bieżącym charakterze, są delegowane na niższe szczeble Pani/Pana komórki organizacyjnej?							
15	Czy został określony ogólny cel istnienia [jednostki] np. w postaci misji (poza statutem lub ustawą powołującą jednostkę)?							
16	Czy w [jednostce] zostały określone cele do osiągnięcia lub zadania do realizacji w bieżącym roku w innej formie niż regulamin organizacyjny czy statut (np. jako plan pracy, plan działalności itp.)?							
17	Czy cele i zadania [jednostki] na bieżący rok mają określone mierniki, wskaźniki bądź inne kryteria, za pomocą których można							

	<p> sprawdzić czy cele i zadania zostały zrealizowane? - należy odpowiedzieć tylko w przypadku, gdy odpowiedź na pytanie nr 16 brzmi TAK</p>							
18	<p> Czy Pani/Pan wyznacza cele do osiągnięcia i zadania do zrealizowania przez pracowników Pani/Pana komórki organizacyjnej w bieżącym roku?</p>							
19	<p> Czy na bieżąco monitoruje Pani/Pan stan zaawansowania realizacji powierzonych pracownikom zadań?</p>							
20	<p> Czy przygotowuje Pani/Pan okresowe informacje nt. stopnia realizacji powierzonych do wykonania zadań?</p>							
21	<p> Czy w Pani/Pana komórce organizacyjnej w udokumentowany sposób identyfikuje się zagrożenia/ryzyka, które mogą przeszkodzić w realizacji celów i zadań komórki organizacyjnej (np. poprzez sporządzanie</p>							

	<p>rejestr ryzyka lub innego dokumentu zawierającego zidentyfikowane zagrożenia/ryzyka)? (jeśli TAK - proszę przejść do następnym pytań, jeśli NIE proszę przejść do pytania nr 25)</p>							
22	<p>Czy w przypadku każdego ryzyka został określony poziom ryzyka, jaki można zaakceptować?</p>							
23	<p>Czy wśród zidentyfikowanych zagrożeń/ryzyk wskazuje się zagrożenia/ryzyka istotne, które w znaczący sposób mogą przeszkodzić w realizacji celów i zadań Pani/Pana komórki organizacyjnej?</p>							
24	<p>Czy w stosunku do każdego istotnego ryzyka został określony sposób radzenia sobie z tym ryzykiem (tzw. reakcja na ryzyko)?</p>							
25	<p>Czy pracownicy w Pani/Pana komórce organizacyjnej mają bieżący dostęp do</p>							

	procedur/instrukcji obowiązujących w [jednostce] (np. poprzez intranet)?							
26	Czy w [jednostce] zostały zapewnione mechanizmy (procedury) służące utrzymaniu ciągłości działalności na wypadek awarii (np. pożaru, powodzi, poważnej awarii)? (jeśli TAK - proszę przejść do następnego pytania, jeśli NIE proszę przejść do pytania nr 28)							
27	Czy pracownicy Pani/Pana komórki organizacyjnej zostali zapoznani z mechanizmami (procedurami) służącymi utrzymaniu działalności na wypadek awarii?							
28	Czy w Pani/Pana komórce organizacyjnej są ustalone zasady zastępstw zapewniających sprawną pracę komórki w przypadku nieobecności poszczególnych pracowników?							

29	Czy Pani/Pana zdaniem istnieje sprawny przepływ informacji wewnątrz Pani/Pana komórki organizacyjnej?							
30	Czy Pani/Pana zdaniem istnieje sprawny przepływ informacji pomiędzy poszczególnymi komórkami organizacyjnymi w [jednostce]?							
31	Czy w [jednostce] funkcjonuje efektywny system wymiany ważnych informacji z podmiotami zewnętrznymi (np. z innymi urzędami, dostawcami, klientami) mającymi wpływ na osiągnięcie celów i realizację zadań Pani/Pana komórki organizacyjnej?							
32	Czy Pani/Pana komórka organizacyjna utrzymuje efektywne kontakty z podmiotami zewnętrznymi, które mają wpływ na realizację jej zadań (np. z innymi urzędami, dostawcami, klientami)?							

33	Czy pracownicy w Pani/Pana komórce organizacyjnej zostali poinformowani o zasadach obowiązujących w [jednostce] w kontaktach z podmiotami zewnętrznymi (np. wnioskodawcami, dostawcami, oferentami)?							
34	Czy zachęca Pani/Pan pracowników do sygnalizowania problemów i zagrożeń w realizacji powierzonych im zadań?							
35	Czy praca audytu wewnętrznego przyczynia się, Pani/Pana zdaniem, do lepszego funkcjonowania [jednostki]?							

Załącznik Nr 1 do zasad samooceny systemu kontroli zarządczej w Starostwie Powiatowym

Kwestionariusz samooceny kontroli zarządczej – pracownik jednostki

	PYTANIE	TAK	Odpowiedź TAK Dowody	NIE	Odpowiedź przyczyny NIE-	Trudno ocenić	Odpowiedź trudno ocenić - przyczyny	Uwagi (propozycje)
1	Czy Pani/Pan wie jakie zachowania pracowników uznawane są w [jednostce] za nieetyczne?							
2	Czy Pani/Pan wie jak należy się zachować w przypadku, gdy będzie Pani/Pan świadkiem poważnych naruszeń zasad etycznych obowiązujących w [jednostce] ?							
3	Czy Pani/Pana zdaniem osoby na stanowiskach kierowniczych przestrzegają i promują własną postawą i decyzjami etyczne postępowanie?							
4	Czy bierze Pani/Pan udział w szkoleniach w wystarczającym stopniu, aby skutecznie realizować powierzone zadania?							
5	Czy szkolenia, w których Pan/Pani uczestniczył/a były przydatne na zajmowanym stanowisku?							

6	Czy jest Pani/Pan informowany przez bezpośredniego przełożonego o wynikach okresowej oceny Pani/Pana pracy?							
7	Czy istnieje dokument, w którym zostały ustalone wymagania w zakresie wiedzy, umiejętności i doświadczenia konieczne do wykonywania zadań na Pani/Pana stanowisku pracy (np. zakres obowiązków, opis stanowiska pracy)?							
8	Czy posiada Pani/Pan aktualny zakres obowiązków określony na piśmie lub inny dokument o takim charakterze?							
9	Czy są Pani/Panu znane kryteria, za pomocą których oceniane jest wykonywanie Pani/Pana zadań?							
10	Czy bezpośredni przełożeni w wystarczającym stopniu monitorują na bieżąco stan zaawansowania powierzonych pracownikom zadań?							

1 1	Czy zna Pani/Pan najważniejsze cele istnienia [jednostki]?							
1 2	Czy w Pani/Pana komórce organizacyjnej zostały określone cele do osiągnięcia lub zadania do realizacji w bieżącym roku w innej formie niż regulamin organizacyjny (np. jako plan pracy, plan działalności itp.)?							
1 3	Czy cele i zadania Pani/Pana komórki organizacyjnej na bieżący rok mają określone mierniki, wskaźniki bądź inne kryteria, za pomocą których można sprawdzić czy cele i zadania zostały zrealizowane? - należy odpowiedzieć tylko w przypadku, gdy odpowiedź na pytanie nr 12 brzmi TAK							
1 4	Czy w Pani/Pana komórce organizacyjnej w udokumentowany sposób identyfikuje się zagrożenia/ryzyka, które mogą przeszkodzić w realizacji celów i zadań komórki organizacyjnej (np. poprzez sporządzanie							

	rejestru ryzyka lub innego dokumentu zawierającego zidentyfikowane zagrożenia/ryzyka)?							
1 5	Czy wśród zidentyfikowanych zagrożeń/ryzyk wskazuje się zagrożenia/ryzyka istotne, które w znaczący sposób mogą przeszkodzić w realizacji celów i zadań komórki organizacyjnej?							
1 6	Czy w Pani/Pana komórce organizacyjnej podejmuje się wystarczające działania mające na celu ograniczenie zidentyfikowanych zagrożeń/ryzyk, w szczególności tych istotnych?							
1 7	Czy posiada Pani/Pan bieżący dostęp do procedur/instrukcji obowiązujących w [jednostce] (np. poprzez intranet)?							
1 8	Czy istniejące procedury w wystarczającym stopniu opisują zadania realizowane przez Panią/Pana?							
1 9	Czy obowiązujące Panią/Pana procedury/instrukcje są							

	aktualne, tzn. zgodne z obowiązującymi przepisami prawa i regulacjami wewnętrznymi (np. regulaminem organizacyjnym, innymi procedurami)?							
20	Czy nadzór ze strony przełożonych zapewnia skuteczną realizację zadań?							
21	Czy wie Pani/Pan jak postępować w przypadku wystąpienia sytuacji nadzwyczajnej np. pożaru, powodzi, poważnej awarii?							
22	Czy w Pani/Pana komórce organizacyjnej są ustalone zasady zastępstw na Pani/Pana stanowisku pracy?							
23	Czy dokumenty/materiały/zasoby informatyczne, z których korzysta Pani/Pan w swojej pracy są Pani/Pana zdaniem odpowiednio chronione przed utratą lub zniszczeniem?							
24	Czy ma Pani/Pan dostęp do wszystkich informacji i danych niezbędnych do realizacji powierzonych Pani/Panu zadań?							

2 5	Czy postawa osób na stanowiskach kierowniczych w Pani/Pana komórce organizacyjnej zachęca pracowników do sygnalizowania problemów i zagrożeń w realizacji zadań komórki organizacyjnej?							
2 6	Czy w przypadku wystąpienia trudności w realizacji zadań zwraca się Pani/Pan w pierwszej kolejności do bezpośredniego przełożonego z prośbą o pomoc?							
2 7	Czy Pani/Pana zdaniem istnieje sprawny przepływ informacji wewnątrz Pani/Pana komórki organizacyjnej?							
2 8	Czy Pani/Pana zdaniem istnieje sprawny przepływ informacji pomiędzy poszczególnymi komórkami organizacyjnymi w [jednostce]?							
2 9	Czy zna Pani/Pan zasady kontaktów pracowników [jednostki] z podmiotami zewnętrznymi (np.							

	wnioskodawcami, dostawcami, oferentami) oraz swoje uprawnienia i obowiązki w tym zakresie?							
3 0	Czy Pani/Pana komórka organizacyjna utrzymuje efektywne kontakty z podmiotami zewnętrznymi, które mają wpływ na realizację jej zadań (np. z innymi urzędami, dostawcami, klientami)?							
3 1	Czy przełożeni na co dzień zwracają wystarczającą uwagę na przestrzeganie przez pracowników obowiązujących w [jednostce] zasad, procedur, instrukcji itp.?							

STAROSTA KĘPIŃSKI
/-/ ROBERT KIERUZAL

Uzasadnienie
do Zarządzenia Nr 16/2023 Starosty Kępińskiego
z dnia 6 kwietnia 2023r.

Uwzględniając szereg okoliczności, które były przedmiotem oceny funkcjonowania systemu kontroli zarządczej w Starostwie Powiatowym w Kępnie, w tym zalecenia audytu wewnętrznego, należy przyjąć za zasadne wprowadzenie jednego ujednoliczonego zarządzenia regulującego funkcjonowanie całości kontroli zarządczej w Starostwie Powiatowym w Kępnie i Powiecie Kępińskim i uchylenie obecnie obowiązujących zarządzeń. Dotychczasowe zarządzenia charakteryzowały się rozproszeniem materii podlegającej regulacji, wieloma aktami prawnymi o charakterze wewnętrznie obowiązującym, w których powtarzane były tożsame regulacje.

Biorąc pod uwagę powyższe wprowadzenie nowych ujednoliconych regulacji kontroli zarządczej jest w pełni uzasadnione.

STAROSTA KĘPIŃSKI

/-/ ROBERT KIERUZAL