ZARZĄDZENIE NR 13/2019
BURMISTRZA KARCZEWA
z dnia 26 lutego 2019 roku

w sprawie zarządzania ryzykiem w Urzędzie Miejskim w Karczewie i jednostkach organizacyjnych Gminy Karczew

Na podstawie art. 33 ust. 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym z dnia 15 sierpnia 2017 r. (Dz. U. z 2018 r., poz. 994 z póź.zm.[1]) oraz art. 68 ust. 2 pkt. 7 i art. 69 ust. 1 pkt. 2 ustawy z dnia 27 sierpnia 2009 roku o finansach publicznych (Dz. U. z 2017 r. poz. 2077 z póź.zm[2]) a także § 20 ust. 1 i 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), zarządza się, co następuje:

§ 1. 1. Wprowadza się Politykę zarządzania ryzykiem w Urzędzie Miejskim w Karczewie i jednostkach organizacyjnych Gminy Karczew, stanowiący Załącznik Nr 1 do niniejszego Zarządzenia.

2. Przez jednostki organizacyjne Gminy Karczew, do których skierowane jest niniejsze Zarządzenie, rozumie się jednostki budżetowe, zakład budżetowy oraz instytucje kultury, zwanych „Jednostkami Organizacyjnymi".

§ 2. 1. Zarządzenie określa zasady i tryb zarządzania ryzykiem w Urzędzie Miejskim w Karczewie i Jednostkach Organizacyjnych Gminy Karczew.

2. Zarządzenie ma zastosowanie w systemie zarządzania ryzykiem w ramach realizowanych zadań oraz w systemie bezpieczeństwa informacji i ochrony danych osobowych.

§ 3. Traci moc Zarządzenie nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku w sprawie wprowadzenia polityki zarządzania ryzykiem.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Karczewa
mgr Michał Rudzki

[1] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w: Dz.U. z 2018 r., poz. 1000, poz. 1349, poz. 1432 oraz poz. 2500.

[2] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w: Dz.U. z 2018 r., poz. 62; , poz. 1000, poz. 1366, poz. 1669, poz. 1693, poz. 2354 oraz poz. 2500.

ZAŁĄCZNIK
DO ZARZĄDZENIA NR 13/2019
BURMISTRZA KARCZEWA
z dnia 26 lutego 2019 r.

§ 1. Ilekroć w zarządzeniu jest mowa o:

1) **Urząd** - należy przez to rozumieć Urząd Miejski w Karczewie;
2) **Burmistrz**– Burmistrz Karczewa;
3) **Komórkach organizacyjnych** – należy przez to rozumieć wydziały, referaty, samodzielne stanowiska w Urzędzie;
4) **Jednostkach Organizacyjnych** - należy przez to rozumieć jednostki organizacyjne Gminy Karczew do których skierowane jest niniejsze Zarządzenie, w tym: jednostki budżetowe, zakład budżetowy oraz instytucje kultury;
5) **Ryzyku** - należy przez to rozumieć możliwość wystąpienia w przyszłości dowolnego zdarzenia, działania lub zaniechania działania, którego skutkiem może być zagrożenie (szkoda) lub niewykorzystana szansa, wpływające na osiągnięcie wyznaczonych celów/zadań;
6) **Ryzyko w bezpieczeństwie informacji** – należy przez to rozumieć potencjalną sytuację, gdzie określone zdarzenie wykorzysta podatność (słabość) aktywów powodując szkodę w organizacji;
7) **Wpływie ryzyka** - należy przez to rozumieć skutki dla realizowania zadań i osiągania celów spowodowane przez zdarzenie objęte ryzykiem;
8) **Prawdopodobieństwo wystąpienia ryzyka** - należy przez to rozumieć częstotliwość występowania zdarzenia objętego ryzykiem;
9) **Istotności ryzyka** - należy przez to rozumieć kombinację wpływu ryzyka i prawdopodobieństwa jego wystąpienia;
10) **Akceptowanym poziomie ryzyka** - należy przez to rozumieć ustalony w zarządzeniu poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku;
11) **Zarządzaniu ryzykiem** - należy przez to rozumieć proces identyfikacji, oceny i przeciwdziałaniu ryzyku; proces ten obejmuje także monitorowanie ryzyka i środków podejmowanych w celu jego ograniczenia;
12) **Mechanizmach kontroli** - należy przez to rozumieć wszystkie działania i procedury podejmowane lub ustanawiane w celu zwiększenia prawdopodobieństwa realizacji zadań i osiągania celów, w tym zwłaszcza:
    a) dokumentację systemu zarządzania i systemu bezpieczeństwa informacji (procedury, instrukcje, wytyczne),
    b) dokumentowanie poszczególnych zdarzeń,
    c) zatwierdzanie operacji,
    d) podział obowiązków,
    e) nadzór,
    f) rejestrowanie istotnych odstępstw od zasad zapisanych w procedurach, instrukcjach czy wytycznych,
    g) ograniczenie dostępu do zasobów materialnych, finansowych

14) **Aktywach** – należy przez to rozumieć wszystko co ma wartość dla organizacji;

a) Aktywa podstawowe:
- Procesy i działania
- Informacje, w tym dane osobowe;

b) Aktywa wspierające:

- Sprzęt (np. laptop, serwer, komputer, drukarka, dysk wymienny CD ROM, inne nośniki: papier, slajd, mikrofilm, fax)
- Oprogramowanie (np. aplikacje, oprogramowanie systemowe)
- Sieć
- Personel
- Siedziba
- Struktura organizacyjna;

13) **Poufność informacji** – należy przez to rozumieć zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom (tylko uprawnieni pracownicy mają dostęp do informacji),
14) **Integralność informacji** – należy przez to rozumieć zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
15) **Dostępność informacji** – należy przez to rozumieć zapewnienie, że informacje są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot (osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne),
16) **Rozliczalność** – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (możliwość zidentyfikowania użytkownika) odpowiedzialnego za informację, jej przetwarzanie.

§ 2. 1. Celem zarządzania ryzykiem w Urzędzie Miejskim w Karczewie i jednostkach organizacyjnych Gminy jest:
1) usprawnienie procesu planowania;
2) zwiększenie prawdopodobieństwa realizacji zadań i osiągania celów;
3) uzyskanie bezpieczeństwa informacji, w tym danych osobowych;
4) zapewnienie odpowiednich mechanizmów kontroli;
5) zapewnienie kierownictwu Urzędu i Jednostek Organizacyjnych wczesnej informacji o zagrożeniach dla realizacji wyznaczonych celów i zadań.

2. Zarządzanie ryzykiem odbywa się według zasad:
1) integracji z procesem zarządzania;
2) powiązania z celami i zadaniami Urzędu i Jednostek Organizacyjnych;
3) przypisania odpowiedzialności;
4) proporcjonalności działań przeciwdziałających ryzyku do jego istotności.

3. Proces zarządzania ryzykiem w gminie Karczew i jednostkach organizacyjnych jest przedstawiony w Załączniku Nr 1 do polityki zarządzania ryzykiem.

§ 3. 1. W proces zarządzania ryzykiem zaangażowani są wszyscy pracownicy Urzędu i Jednostek Organizacyjnych.

2. Polityka zarządzania ryzykiem określa najistotniejsze zadania:
1) kierownictwa;
2) naczelników wydziałów/samodzielne stanowiska;
3) pracowników;
4) koordynatora kontroli zarządczej;
5) audytora wewnętrznego.

3. Role i odpowiedzialność osób w procesie zarządzania ryzykiem:

Kierownictwo	**Naczelnicy wydziałów/samodzielne stanowiska**	**Pracownicy**
1. Określenie strategicznego podejścia do zarządzania ryzykiem i określenie	1. Budowanie wiedzy na temat ryzyka w ramach podległego obszaru.	1. Zrozumienie, akceptacja oraz wdrożenie założeń procesu zarządzania

akceptowanego poziomu ryzyka. 2. Wdrożenie struktury zarządzania ryzykiem. 3. Zarządzanie najbardziej kluczowymi ryzykami. 4. Zarządzanie jednostką w przypadku kryzysu.	2. Uzgadnianie celów i działań w ramach zarządzania ryzykiem. 3. Zapewnienie wdrożenia rekomendacji z zakresu usprawnienia procesu zarządzania ryzykiem. 4. Identyfikacja i raportowanie o zmianach w katalogu ryzyka komórki organizacyjnej.	ryzykiem. 2. Raportowanie na temat nieefektywnych, nieskutecznych i niepotrzebnych mechanizmów kontrolnych. 3. Współpraca z kierownictwem nad wyjaśnieniem zmaterializowanych ryzyk.

Koordynator kontroli zarządczej	**Audytor wewnętrzny**
1. Opracowanie polityki zarządzania ryzykiem oraz jej aktualizacja. 2. Dokumentowanie struktury oraz polityki zarządzania poszczególnymi ryzykami. 3. Koordynowanie czynności w ramach procesu zarządzania ryzykiem. 4. Dokumentowanie procesu i opracowywanie informacji końcowej dla kierownictwa.	1. Opracowanie programu audytu opartego na analizie ryzyka. 2. Przeprowadzenie audytu procesu zarządzania ryzykiem. 3. Wydawanie oraz otrzymywanie zapewnienia w obszarze zarządzania ryzykami. 4. Raportowanie na temat efektywności i skuteczności mechanizmów kontrolnych.

§ 4. Identyfikacja i ocena ryzyka oraz ustalenie metody przeciwdziałania ryzyku dokonywane jest podczas przygotowywania do realizacji zadań Urzędu i Jednostek Organizacyjnych w danym roku.

§ 5. 1. Identyfikacja ryzyka polega na ustaleniu ryzyka zagrażającego poszczególnym zadaniom i celom realizowanym przez Urząd i Jednostki Organizacyjne oraz na ustaleniu ryzyk zagrażających utracie poufności, integralności, dostępności i rozliczalności aktywów (w tym m.in. informacji, danych osobowych, sprzętu).

2. Podczas identyfikacji należy przeanalizować:

1) zadania i cele proponowane do realizacji w danym roku przez Urząd i Jednostki Organizacyjne;
2) zagrożenia, związane z osiąganiem celów i realizowaniem zadań przez Urząd i Jednostki Organizacyjne, wraz z ich wewnętrznymi i zewnętrznymi przyczynami oraz możliwymi scenariuszami rozwoju zdarzeń;
3) zagrożenia związane z utratą poufności, integralności, rozliczalności i dostępności do informacji i danych, w tym danych osobowych.

3. Podczas identyfikacji stosowana jest kategoryzacja ryzyka.

4. Ustala się następujące kategorie (obszary) ryzyka:

1) ryzyko finansowe;
2) ryzyko dotyczące zasobów ludzkich;
3) ryzyko działalności;
4) ryzyko zewnętrzne;

Przykłady ryzyka występującego w ramach powyższych kategorii stanowi Załącznik Nr 2 do polityki zarządzania ryzykiem.

5. W ramach systemu bezpieczeństwa informacji i danych osobowych ustala się następujące kategorie (obszary) ryzyka:

1) ryzyko naruszenia bezpieczeństwa informacji;
2) ryzyko awarii technicznej;
3) ryzyko nieautoryzowanego działania;

4) ryzyko naruszenia bezpieczeństwa funkcji;
5) ryzyko utraty podstawowych usług;
6) ryzyko zniszczenia fizycznego;
7) ryzyko związane z wystąpieniem zjawiska naturalnego;
Przykłady ryzyka występującego w ramach powyższych kategorii (obszarów) stanowi Załącznik Nr 3 do polityki zarządzania ryzykiem.

§ 6. 1.Ocena ryzyka polega na określeniu wpływu i prawdopodobieństwa ziszczenia się ryzyka, a następnie ustaleniu jego istotności.

2. Określenie wpływu ryzyka polega na ustaleniu przewidywanych skutków jakie będzie miało wystąpienie zdarzenia objętego ryzykiem, dla realizacji zadań lub osiągania celów. Do określenia wpływu używany jest opis jakościowy przy zastosowaniu skali ocen: bardzo wysoki, wysoki, średni, niski oraz ocenę punktową przy zastosowaniu skali od 1 do 4.

Tabela 1. Zasady oceny wpływu ryzyka

Wpływ	**Opis szczegółowy**
Bardzo wysoki 4	✓ rozwiązanie problemu będzie wymagało dużego nakładu czasu i zasobów oraz podjęcia decyzji na poziomie strategicznym, ✓ brak realizacji kluczowych zadań i celów, ✓ paraliż działalności Urzędu i Jednostek Organizacyjnych, ✓ skutki będą nieodwracalne, ✓ bardzo poważne i rozległe konsekwencje prawne, ✓ naruszenie bezpieczeństwa pracowników (ujemne konsekwencje dla ich życia i zdrowia), ✓ straty finansowe w zakresie powyżej 100.000 zł, ✓ utrata dobrego wizerunku jednostki w środowisku oraz w opinii publicznej – negatywne opinie w mediach ogólnopolskich, ✓ naruszenie praw lub wolności osób fizycznych przez brak realizacji praw lub obowiązków wynikających z RODO, ✓ konsekwencje dla osób fizycznych (motyw 85 RODO) – duża skala.
Wysoki 3	✓ rozwiązanie problemu będzie wymagało dużego nakładu czasu i/lub zasobów oraz podjęcia decyzji przez kierownictwo wyższego szczebla o sposobie wyjścia z zaistniałej sytuacji, ✓ poważny wpływ na realizację zadania, w tym poważne zagrożenie terminu jego realizacji jak i osiągnięcia celu, ✓ poważne zakłócenia w działalności Urzędu i Jednostek Organizacyjnych, ✓ usunięcie skutków będzie bardzo trudne, ✓ poważne konsekwencje prawne, ✓ straty finansowe w zakresie powyżej 50.000-100.000 zł, ✓ zagrożenie bezpieczeństwa pracowników, ✓ zagrożenie bezpieczeństwa zasobów (np. utrata danych, nieuprawniony dostęp), ✓ poważny wpływ na wizerunek jednostki – negatywne opinie w mediach krajowych, ✓ naruszenie praw lub wolności osób fizycznych przez brak realizacji praw lub obowiązków wynikających z RODO, ✓ konsekwencje dla osób fizycznych (motyw 85 RODO) – umiarkowana skala.
Średni 2	✓ rozwiązanie problemu będzie wymagało umiarkowanego nakładu czasu i/lub zasobów,

	✓ średni wpływ na realizację celów i zadań, ✓ umiarkowany poziom zakłóceń w działalności Urzędu i Jednostek Organizacyjnych, ✓ usuniecie skutków będzie wymagało czasu, ✓ umiarkowane konsekwencje prawne, ✓ skutek finansowy w zakresie powyżej 10.000-50.000 zł, ✓ brak wpływu na bezpieczeństwo pracowników, ✓ średni wpływ na wizerunek jednostki – negatywne opinie w mediach lokalnych i regionalnych, ✓ naruszenie praw lub wolności osób fizycznych przez opóźnienia w realizacji praw lub obowiązków wynikających z RODO – umiarkowana skala
Niski **1**	✓ rozwiązanie problemu będzie wymagało znikomego nakładu czasu i/lub zasobów, ✓ mały wpływ na realizację celów i zadań, ✓ możliwe jedynie niewielkie zakłócenia w działalności Urzędu i Jednostek Organizacyjnych, ✓ brak trwałej szkody, ✓ brak skutków prawnych, ✓ skutek finansowy w zakresie do 10.000 zł, ✓ brak wpływu na bezpieczeństwo pracowników, ✓ niewielki wpływ na wizerunek jednostki – negatywne opinie bez udziału mediów, ✓ naruszenia praw lub wolności osób fizycznych przez niewielkie opóźnienie w realizacji praw lub obowiązków wynikających z RODO

3. Określenie prawdopodobieństwa ziszczenia się ryzyka polega na ustaleniu przewidywanej częstotliwości występowania zdarzenia objętego ryzykiem w trakcie roku. Do określenia prawdopodobieństwa stosowany jest opis jakościowy przy zastosowaniu skali ocen: bardzo wysokie, wysokie, średnie, niskie oraz ocenę punktową przy zastosowaniu skali od 1 do 4.

Tabela 2. Zasady oceny stopnia prawdopodobieństwa ziszczenia się ryzyka

Prawdopodobieństwo	**Opis szczegółowy**
Bardzo wysokie **4**	Zdarzenie wystąpi w najbliższym terminie – lub co najmniej raz w tygodniu
Wysokie **3**	Zdarzenie występuje wielokrotnie w ciągu roku -co najmniej raz w miesiącu
Średnie **2**	Zdarzenie występuje więcej niż raz w roku -co najmniej raz na kwartał
Niskie **1**	✓ Do tej pory takie zdarzenie nie wystąpiło w Urzędzie lub w Jednostkach Organizacyjnych lub może zaistnieć jedynie w wyjątkowych okolicznościach raz w roku

§ 7. 1. W oparciu o dokonaną ocenę wpływu i prawdopodobieństwa ziszczenia się ryzyka ustalany jest poziom istotności ryzyka:

2. Określenie prawdopodobieństwa (P) i wpływu ryzyka (W) w czterostopniowej skali, umożliwia ustalenie współczynnika istotności ryzyka (IR) – jako iloczynu (wyrażonych punktowo) prawdopodobieństwa wystąpienia ryzyka (P) oraz potencjalnego wpływu jego wystąpienia (W):

IR = P x W
gdzie:
IR – współczynnik istotności ryzyka
P – prawdopodobieństwo wystąpienia ryzyka
W – potencjalny wpływ ryzyka

3. Po przeprowadzonej analizie, wartości przyporządkowane, zarówno wpływów i jak i prawdopodobieństwu ryzyka, należy przenieść na mapę ryzyka. Mapę punktowej oceny istotności ryzyka „4 x4", przedstawiono poniżej:

Mapa ryzyka 4x4

Oddziaływanie					
Bardzo wysokie	4 niskie	8 średnie	12 wysokie	16 bardzo wysokie	
Wysokie	3 niskie	6 średnie	9 wysokie	12 wysokie	
Średnie	2 niskie	4 niskie	6 średnie	8 średnie	
Niskie	1 niskie	2 niskie	3 niskie	4 niskie	
	Niskie	**Średnie**	**Wysokie**	**Bardzo wysokie**	**Prawdopodobieństwo**

§ 8. 1. **Istotność ryzyka** obliczona według wzoru umożliwia dokonanie oceny i hierarchizacji ryzyka.

2. Dla oceny istotności ryzyka stosuje się trzystopniową skalę obejmującą następujące poziomy:

- **WYSOKI** – jest to ryzyko o wartości 9-16, które istotnie wpływa na kluczową działalność jednostki, uniemożliwia realizację jej zadań i celów, rodzi straty finansowe,
- **ŚREDNI** – jest to ryzyko o wartości 6-8, które potencjalnie wpływa na kluczową działalność jednostki, jest zagrożeniem dla realizacji zadań i celów, zagraża powstaniem strat finansowych,
- **NISKI** – jest to ryzyko o wartości 1–4, które nie ma wpływu na kluczową działalność jednostki, nie uniemożliwia realizacji zadań i osiągania celów.

Poziomy istotności	**Wartość punktowa**	**Przesłanki**
Niski	1 -4	Ryzyko akceptowalne
		Akceptacja - ryzyko podlega minimalnemu monitorowaniu. Wartość

		ryzyka powinna zostać zweryfikowana dopiero przy następnej analizie lub gdy zmienią się warunki mające wpływ na podniesienie wartość ryzyka.
Średni	6-8	Ryzyko możliwe do zaakceptowania.
		Działanie ograniczające ryzyko do poziomu akceptowalnego. Należy rozważyć możliwość przeniesienia ryzyka na inny podmiot. Ryzyko wymaga monitorowania oraz zaplanowania i podjęcia działań prewencyjnych w określonym dłuższym okresie czasu (w zależności od możliwości np. w ciągu kwartału, półrocza czy roku), przy czym dopuszcza się akceptację ryzyka z tego przedziału, gdyby szacowane koszty niezbędnych działań przewyższały korzyści z ograniczenia ryzyka lub właściciel ryzyka podwyższył jego akceptowalny poziom. W sytuacji akceptacji takiego ryzyka właściciel ryzyka powinien monitorować ryzyko i okresowo rozważać potrzebę podjęcia działań ograniczających ryzyko.
Wysoki	9-16	Ryzyko nieakceptowane. Działanie niezwłoczne – ryzyko wymaga niezwłocznego podjęcia działań ograniczających ryzyko. Należy rozważyć możliwość przeniesienia ryzyka na inny podmiot lub jeśli jest to możliwe wycofania się z realizacji zadania powodującego ryzyko.

2. Metodami przeciwdziałania ryzyku są;

1) **kontrolowanie ryzyka** - podejmowanie działań zaradczych pozwalających na ograniczenie ryzyka do akceptowanego poziomu m. in. poprzez wzmocnienie mechanizmów kontroli wewnętrznej, w tym zwłaszcza procedury, instrukcje, upoważnienia, podział obowiązków, nadzór, szkolenia;
2) **akceptacja** - zaniechanie podejmowania działań zaradczych z uwagi na brak możliwości wskazania takich działań, które byłyby skuteczne lub w przypadku, gdy koszt podjętych działań zaradczych jest wyższy niż koszt poniesienia ryzyka;
3) **przeniesienie ryzyka** - przekazanie ryzyka podmiotowi zewnętrznemu np. w drodze ubezpieczenia, zlecenie wykonania usługi;
4) **unikanie** – zaprzestanie/zawieszenie działań rodzących zbyt duże ryzyko;

3. W celu określenia metody przeciwdziałania ryzyku należy przeanalizować:

1) przyczyny (źródła) ryzyka i możliwe scenariusze rozwoju wydarzeń;
2) istniejące mechanizmy kontroli stosowane w celu ograniczenia lub uniknięcia tego ryzyka;
3) skuteczność istniejących mechanizmów kontroli, tj. zakres w jakim przeciwdziałają ryzyku, a poprzez to ułatwiają lub utrudniają realizację ustalonych celów i zadań.

§ 9. 1. Kierownicy komórek organizacyjnych Urzędu oraz kierownicy Jednostek Organizacyjnych dokonują wyboru obszarów ryzyka wskazanych w Załączniku Nr 4 oraz dokonują identyfikacji ryzyka, oceny ryzyka oraz określenia metod przeciwdziałania ryzyku, według wzoru zamieszczonego w Załączniku Nr 5 do polityki zarządzania ryzykiem.

2. W ramach systemu bezpieczeństwa informacji i danych osobowych, kierownicy komórek organizacyjnych Urzędu, oraz kierownicy Jednostek Organizacyjnych identyfikują aktywa organizacji do zagrożeń (utrata poufności, integralności, dostępności, rozliczalności), identyfikują ryzyka oraz wskazują stosowane w komórce organizacyjnej zabezpieczenia techniczne i organizacyjne, a następnie dokonują szacowania ryzyka, według wzoru stanowiącego Załącznik Nr 6 do polityki zarządzania ryzykiem.

3. Arkusze przedkładane są do dnia 31 stycznia każdego roku (w 2019 roku do 15 marca),

1) koordynatorowi kontroli zarządczej w zakresie zidentyfikowanych ryzyk dotyczących realizacji zadań i celów przez Urząd i Jednostki Organizacyjne,
2) Inspektorowi Ochrony Danych w zakresie zidentyfikowanych ryzyk w bezpieczeństwie informacji i danych osobowych.

4. Koordynator kontroli zarządczej i Inspektor Ochrony Danych przekazują Burmistrzowi Karczewa informację o najistotniejszych ryzykach zagrażających realizacji celów i zadań komórek organizacyjnych Urzędu Jednostek Organizacyjnych, w formie rejestru ryzyk, stanowiący Załącznik Nr 7 i Nr 8 do polityki zarządzania ryzykiem.

§ 10. 1. Kierownicy komórek organizacyjnych i kierownicy jednostek organizacyjnych zapewniają stosowanie metod przeciwdziałania ryzyku ustalonych w Arkuszach.

2. Przynajmniej raz w roku należy dokonać przeglądu ryzyk wpisanych do ww. arkuszy.

3. W wyniku przeglądu mogą zostać usunięte z arkusza znajdujące się w nim ryzyka lub zostać wprowadzone nowe. Może również ulec zmianie istotność ryzyka oraz sposoby reakcji na nie.

§ 11. 1. Zidentyfikowane ryzyko oraz ustalone metody jego ograniczania do akceptowanego poziomu są na bieżąco oceniane (monitorowane) przez:

1) Naczelników wydziałów / samodzielne stanowiska i kierowników jednostek organizacyjnych, którzy oceniają poziom zidentyfikowanego ryzyka oraz skuteczność stosowanych metod jego ograniczania;
2) Inspektora Ochrony Danych w zakresie bezpieczeństwa informacji, danych osobowych w ramach audytów ochrony danych osobowych i bezpieczeństwa informacji;
3) Burmistrza Karczewa lub jego Zastępca w ramach bieżącego zarządzania Urzędem, w tym w szczególności w trakcie narad z naczelnikami i kierownikami jednostek organizacyjnych.

2. Efektywność zarządzania ryzykiem oraz system kontroli podlega niezależnej i obiektywnej ocenie przez audyt wewnętrzny oraz wewnętrzny audyt bezpieczeństwa informacji.

3. Wyniki oceny, o której mowa w ust. 1 i 2, wykorzystywane są do poprawy efektywności zarządzania ryzykiem oraz usprawnienia systemu zarządzania Urzędem i Jednostek Organizacyjnych.

Burmistrz Karczewa
mgr Michał Rudzki

ZAŁĄCZNIK NR 1
do polityki
zarządzania
ryzykiem

PROCES ZARZĄDZANIA RYZYKIEM W GMINIE KARCZEW i JEDNOSTKACH ORGANIZACYJNYCH

MIERNIKI

1) **Precyzyjne** - zwięzłe i jednoznaczne
2) **Mierzalne** - właściwe mierniki i wskaźniki
3) **Osiągalne**
4) **Istotne**
5) **Określone w czasie**

ZADANIA STRATEGICZNE

ZADANIA OPERACYJNE

IDENTYFIKACJA RYZYKA

RYZYKO- możliwość wystąpienia w przyszłości dowolnego zdarzenia, działania lub

ANALIZA I OCENA

		Oddziaływanie	Prawdopodobieństwo			
Poważne zagrożenie dla działalności lub osiągnięcia celów działania	**4** bardzo wysokie		4	8	12	16
Poważny wpływ na cele i zadania, poważny uszczerbek w zakresie jakości, duża strata finansowa	**3** wysokie		3	6	9	12
Strata posiadanych zasobów, negatywny (średni) wpływ na efektywność działania	**2** średnie		2	4	6	8
Niewielka strata finansowa lub opóźnienie	**1** niskie		1	2	3	4

REAKCJA I OGRANICZANIE

Poziom istotności		Działania
wysoki	9-16	Działanie natychmiastowe, silne mechanizmy kontroli, ciągły monitoring.
średni	5-8	Monitorowanie i rozważenie potrzeby działań zaradczych oraz wprowadzenia dodatkowych mechanizmów kontroli.
niski	1-4	Stały monitoring, ryzyko akceptowane.

METODY REAKCJI NA RYZYKO:

1) tolerowanie
2) transfer

PRZECIWDZIAŁANIE RYZYKU:

1) przyczyny (źródła) i możliwe scenariusze wydarzeń

MONITOROWANIE I RAPORTOWANIE

MONITOROWANIE

1) czy ryzyko nadal istnieje
2) czy pojawiło się nowe
3) czy zmieniło się prawdopodo

SPRAWOZDANIE

1) zadanie planowane a podjęte
2) planowana wartość

zaniechania działania, którego skutkiem może być zagrożenie (szkoda) lub niewykorzystana szansa, wpływające na osiągnięcie wyznaczonych celów/zadań.								3) przeciwdziałanie 4) przesunięcie w czasie (unikanie)	2) istniejące mechanizmy kontroli 3) skuteczność istniejących mechanizmów kontroli	bieństwo i wpływ 4) czy stosowane mechanizmy kontroli są efektywne	miernika a osiągnięta
		Skala		**1** niskie	**2** średnie	**3** wysokie	**4** bardzo wysokie				
	Opis			1 raz w roku lub wcale	Więcej niż 1 raz w roku	Wielokrotnie w ciągu roku	W najbliższym terminie				

ZAŁĄCZNIK NR 2
do polityki zarządzania ryzykiem

Kategorie ryzyka

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

Ryzyko finansowe	
Budżetowe	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów
Podlegające ubezpieczeniu	Związane ze stratami finansowymi, które mogą być przedmiotem ubezpieczenia np. ryzyko pożaru, wypadku
Zamówień publicznych i zlecania zadań publicznych	Związane z podejmowaniem decyzji oraz udzielaniem zamówień publicznych lub zlecaniem zadań publicznych innym podmiotom np. ryzyko naruszenia zasad, form lub trybu ustawy o zamówieniach publicznych
Odpowiedzialności	Związane z obowiązkiem zapłaty kwot pieniężnych tytułem np. odszkodowań, odsetek karnych, kosztów procesowych
Realizacja programów współfinansowanych ze środków UE	Związane z wystąpieniem nieprawidłowości przy wykorzystaniu środków z UE
Ryzyko dot. zasobów ludzkich	
Personelu	Związane z liczebnością i kompetencjami pracowników, szkoleniami, wprowadzaniem nowych zadań bez zabezpieczenia etatowego
Bhp	Związane ze zdrowiem pracowników i wypadkami przy pracy
Ryzyko działalności	
Regulacji wewnętrznych	Związane z istnieniem i adekwatnością regulacji wewnętrznych
Organizacji i podejmowania decyzji	Związane ze strukturą organizacyjną, organizacją pracy oraz przekazywaniem obowiązków i uprawnień np. ryzyko nieprecyzyjnie określonych obowiązków, ryzyko braku formalnie powierzonych obowiązków, ryzyko nieodpowiedniej struktury organizacyjnej, ryzyko nieprawidłowo wydanej decyzji, zapewnienie terminowego ogłaszania aktów normatywnych, w tym przepisów prawa miejscowego
Kontroli wewnętrznej	Związane z funkcjonowaniem systemu kontroli wewnętrznej np. ryzyko niedostatecznej kontroli, ryzyko nieskutecznych mechanizmów kontroli
Informacji	Związane z jakością informacji na podstawie których podejmowane są decyzje np. ryzyko braku komunikacji wewnętrznej i zewnętrznej
Reputacji	Związane z reputacją Urzędu i Jednostek Organizacyjnych np. ryzyko negatywnych opinii
Systemów informatycznych	Związane z używanymi w Urzędzie i Jednostkach Organizacyjnych systemami i programami informatycznymi oraz ochroną zawartych w nich danych np. ryzyko awarii, ryzyko udostępnienia danych osobom nieuprawnionym, ryzyko nieuprawnionej modyfikacji

	danych
Ryzyko zewnętrzne	
Infrastruktury	Związane z infrastrukturą np. wyposażeniem, bazą lokalową, środkami transportu i środkami łączności
Gospodarcze	Związane z czynnikami ekonomicznymi np. kursy walut, inflacja
Środowiska prawnego	Związane ze skomplikowaniem i zmianami prawa oraz niejednolitym orzecznictwem

ZAŁĄCZNIK NR 3
do polityki zarządzania ryzykiem

Kategorie ryzyka

w ramach systemu bezpieczeństwa informacji i danych osobowych

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

Ryzyko naruszenia bezpieczeństwa informacji
Związane z kradzieżą urządzeń, nośników lub dokumentów, ujawnieniem danych, pobieraniem danych z niewiarygodnych źródeł, manipulowaniem urządzeniem oraz sfałszowaniem oprogramowania
Ryzyko awarii technicznej
Związane z awarią urządzenia, niewłaściwym funkcjonowaniem urządzeń, przeciążeniem systemu informacyjnego, niewłaściwym funkcjonowaniem oprogramowania, naruszeniem zdolności utrzymania systemu informacyjnego
Ryzyko nieautoryzowanego działania
Związane z nieautoryzowanym użyciem urządzeń, nieuprawnionym kopiowaniem oprogramowania, użyciem fałszywego lub skopiowanego oprogramowania, zniekształceniem danych, nielegalnym przetwarzaniem danych
Ryzyko naruszenia bezpieczeństwa funkcji
Związane z błędem użytkownika, naruszeniem i fałszowaniem praw
Ryzyko utraty podstawowych usług
Związanego z utratą dostaw prądu, awarią systemu klimatyzacji (serwerownia), awarią urządzenia telekomunikacyjnego

ZAŁĄCZNIK NR 4
do polityki zarządzania ryzykiem

Obszary działalności w Gminie Karczew

Poniższa tabela przedstawia obszary działalności

Nr obszaru działalności	Obszar działalności
1	Zarzadzanie strukturami samorządowymi
2	Organizowanie i wspófinansowanie systemu transportowo-komunikacyjnego na terenie gminy
3	Gospodarki gruntami i nieruchomościami
4	Zrównoważony ład przestrzenny -zagospodarowanie przestrzenne gminy
5	Zadania zlecone z zakresu administracji rządowej
6	Budowa (remonty) infrastruktury drogowej na terenie Gminy Karczew
8	Gospodarowanie mieszkaniowym zasobem gminy
9	Finanse i różne rozliczenia
10	Dostęp do edukacji
11	Dostęp do opieki i wychowania
-	**Wyodrębnione fundusze do dyspozycji mieszkańców, w tym:**
13	Fundusze sołeckie
14	Budżet partycypacyjny
15	Gminny Program Profilaktyki i Rozwiązywania Problemów Alkoholowych i Przeciwdziałania Narkomanii
16	Gminna strategia rozwiązywania problemów społecznych- pomoc społeczna
17	Pomoc środowiskowa osobom z zaburzeniami psychicznymi i ich rodzinom
18	Utrzymanie czystości i porządku na terenie gminy
19	Komunikacja społeczna, w tym promocja gminy
20	Planowanie energetyczne na szczeblu lokalnym -zaopatrzenie społeczności lokalnej w ciepło, energię elektryczną
21	Zarzadzanie ochroną środowiska
12	Wpływy i wydatki związane z gromadzeniem środków z opłat i kar za korzystanie ze środowiska
24	System gospodarowania odpadami komunalnymi
22	Bezpieczeństwo i porządek publiczny
7	Ochotnicze straże pożarne
23	Profilaktyka i promocja zdrowia
25	Kultura u podstaw
26	Organizacja sportu, rekreacji i turystyki
27	Pozyskiwanie zewnętrznych środków finansowych -programy finansowane z udziałem środków zewnętrznych
28	Kontynuacja projektów ze środków zewnętrznych
29	Program Partnerstwo Publiczno - Prywatne -kontynuacja projektów PPP
30	Gospodarka wodno-kanalizacyjna

ZAŁĄCZNIK NR 5
do polityki zarządzania ryzykiem

ARKUSZ IDENTYFIKACJI, OCENY ORAZ OKREŚLENIA METODY PRZECIWDZIAŁANIA RYZYKU

Ryzyko				**Przeciwdziałanie ryzyku**			
L.p.	Obszar działalności (ryzyka)	Cel	Ryzyko (wskazać występujące kategorie ryzyka)	Wpływ (wskazać jedną z ocen)	Prawdopodobieństwo (wskazać jedną z ocen)	Istotność ryzyka kol.5 x kol.6 (proszę zaznaczyć kolorem czerwonym ryzyka wysokie)	Planowana metoda przeciwdziałania ryzyku (działania zaradcze ograniczające ryzyko)
1	2	3	4	5	6	7	8
	np. Gospodarki gruntami i nieruchomościami						

.....
podpis Kierownika

Zasady wypełniania arkusza:

Nr kolumny	**Sposób wypełnienia**
1	Numer kolejny celu lub zadania na dany roku pracy Urzędu i Jednostek Organizacyjnych
2	Obszar działalności (ryzyka)
3	Nazwa celu lub zadania na dany rok pracy Urzędu i Jednostek Organizacyjnych
4	Wskazanie kategorii ryzyka oraz krótki opis jego natury np. ryzyko finansowe związane z nieterminowym regulowaniem płatności
5	Ocena wpływu w skali :- bardzo wysoki- wysoki – średni – niski
6	Ocena prawdopodobieństwa w skali:- bardzo wysoki- wysokie – średnie – niskie
7	Poziom istotności ryzyka wynikający z przyznanych ocen prawdopodobieństwa i wpływu : iloczyn kolumn 5 i 6
8	Wskazanie planowanej metody przeciwdziałania ryzyku np. powierzenie odpowiedzialności wyznaczonemu pracownikowi, bieżący nadzór Naczelnika

ZAŁĄCZNIK NR 6
do polityki zarządzania ryzykiem

ARKUSZ IDENTYFIKACJI, OCENY ORAZ OKREŚLENIA METODY PRZECIWDZIAŁANIA RYZYKU
W ramach systemu bezpieczeństwa informacji i danych osobowych

Ryzyko					**Przeciwdziałanie ryzyku**		
L.p.	Obszar działalności (ryzyka)	Cel	Ryzyko (wskazać występujące kategorie ryzyka)	Wpływ (wskazać jedną z ocen)	Prawdopodobieństwo (wskazać jedną z ocen)	Istotność ryzyka kol.5 x kol.6 (proszę zaznaczyć kolorem czerwonym ryzyka wysokie)	Planowana metoda przeciwdziałania ryzyku (działania zaradcze ograniczające ryzyko)
1	2	3	4	5	6	7	8
	np. Gospodarki gruntami i nieruchomościami						

.....
podpis Kierownika

Zasady wypełniania arkusza:

Nr kolumny	**Sposób wypełnienia**
1	Numer kolejny celu lub zadania na dany roku pracy Urzędu i Jednostek Organizacyjnych
2	Obszar działalności (ryzyka)
3	Nazwa celu zadania na dany rok pracy Urzędu i Jednostek Organizacyjnych
4	Wskazanie kategorii ryzyka oraz krótki opis jego natury np. ryzyko finansowe związane z nieterminowym regulowaniem płatności
5	Ocena wpływu w skali :- bardzo wysoki- wysoki – średni – niski
6	Ocena prawdopodobieństwa w skali:- bardzo wysoki- wysokie – średnie – niskie
7	Poziom istotności ryzyka wynikający z przyznanych ocen prawdopodobieństwa i wpływu : iloczyn kolumn 5 i 6
8	Wskazanie planowanej metody przeciwdziałania ryzyku np. powierzenie odpowiedzialności wyznaczonemu pracownikowi, bieżący nadzór Naczelnika

ZAŁĄCZNIK NR 7
do polityki zarządzania ryzykiem

Rejestr ryzyk na rok ……

L. p.	Obszar działalności (ryzyka)	**Ryzyko***	**komórka organizacyjna lub osoba zarządzająca ryzykiem**	**Reakcja na ryzyko** (działania jakie należy podjąć dla ograniczenia/usunięcia ryzyka)
1	2	3	4	5
1	Obszar działalności np. Gospodarki gruntami i nieruchomościami			
2				
3				

Skala ryzyka: bardzo wysokie i wysokie
Rejestr sporządzono na podstawie arkuszy identyfikacji, oceny oraz określenia metod przeciwdziałaniu ryzyku poszczególnych komórek organizacyjnych.

……

podpis: Koordynator kontroli zarządczej

ZAŁĄCZNIK Nr 8
do polityki zarządzania ryzykiem

Rejestr ryzyk w ramach systemu bezpieczeństwa informacji i danych osobowych

L. p.	Obszar działalności (ryzyka)	**Ryzyko***	**(komórka organizacyjna lub osoba zarządzająca ryzykiem**	**Reakcja na ryzyko** (działania jakie należy podjąć dla ograniczenia/usunięcia ryzyka)
1	2	3	4	5
1	Obszar działalności np. Gospodarki gruntami i nieruchomościami			
2				
3				

*Skala ryzyka: bardzo wysokie i wysokie
Rejestr sporządzono na podstawie arkuszy identyfikacji, oceny oraz określenia metod przeciwdziałaniu ryzyku poszczególnych komórek organizacyjnych.

……
podpis: Inspektora Ochrony Danych