

ZARZĄDZENIE NR 1398/2018

Prezydenta Miasta Sopotu

z dnia 4 lipca 2018 roku

w sprawie zarządzania ryzykiem w Urzędzie Miasta Sopotu i Jednostkach Organizacyjnych Miasta

Na podstawie art. 33 ust. 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym tj. z 15.08.2017 r.(Dz.U. z 2017 r. poz. 1875 ze zm.) 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) 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),

zarządzam, co następuje:

§ 1

1. Zarządzenie określa zasady i tryb zarządzania ryzykiem w Urzędzie Miasta Sopotu i Jednostkach Organizacyjnych Miasta.
2. Zarządzenie ma zastosowanie w systemie zarządzania ryzykiem w ramach realizowanych zadań oraz w systemie bezpieczeństwa informacji i ochrony danych osobowych.

2. Ilekcioć w zarządzeniu jest mowa o:

- 1) **Urząd** - należy przez to rozumieć Urząd Miasta Sopotu;
- 2) **Prezydent** – Prezydent Miasta Sopotu,
- 3) **Sekretarz** – Sekretarz miasta Sopotu,
- 4) **Komórkach organizacyjnych** – należy przez to rozumieć wydziały, referaty, biura, samodzielne stanowiska w Urzędzie Miasta Sopotu;
- 5) **Jednostkach organizacyjnych** - należy przez to rozumieć jednostki organizacyjne Miasta Sopotu;
- 6) **Ryzyku** - należy przez to rozumieć prawdopodobieństwo wystąpienia zdarzenia mającego negatywny wpływ na wykonywanie zadań bądź osiągnięcie celów;
- 7) **Ryzyko w bezpieczeństwie informacji** – należy przez to rozumieć potencjalną sytuację, gdzie określone zdarzenie wykorzysta podatność (słabość) aktywów powodując szkodę w organizacji;
- 8) **Wpływie ryzyka** - należy przez to rozumieć skutki dla realizowania zadań i osiągnięcia celów spowodowane przez zdarzenie objęte ryzykiem;

- 9) **Prawdopodobieństwo wystąpienia ryzyka** - należy przez to rozumieć częstotliwość występowania zdarzenia objętego ryzykiem;
- 10) **Istotności ryzyka** - należy przez to rozumieć kombinację wpływu ryzyka i prawdopodobieństwa jego wystąpienia;
- 11) **Akceptowanym poziomie ryzyka** - należy przez to rozumieć ustalony w zarządzeniu poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku;
- 12) **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;
- 13) **Mechanizmach kontroli** - należy przez to rozumieć wszystkie działania i procedury podejmowane lub ustanawiane w celu zwiększenia prawdopodobieństwa realizacji zadań i osiągnięcia 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

Aktywa podstawowe:

- Procesy i działania
- Informacje, w tym dane osobowe

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 Miasta Sopotu i jednostkach organizacyjnych Miasta jest:

- 1) usprawnienie procesu planowania;
- 2) zwiększenie prawdopodobieństwa realizacji zadań i osiągnięcia 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 obejmuje:

- 1) identyfikację i ocenę ryzyka oraz odniesienie go do akceptowanego poziomu ryzyka;
- 2) ustalenie metody przeciwdziałania ryzyku;
- 3) przeciwdziałanie ryzyku;
- 4) monitorowanie procesu i dokonywanie zmian.

§ 4

1. 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 celom i zadaniom 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) cele i zadania 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 1 do zarządzenia

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 2 do zarządzenia.

§ 6

1. Ocena ryzyka polega na określeniu wpływu i prawdopodobieństwa wystąpienia ryzyka, a następnie ustaleniu jego istotności według zasad określonych w § 7.
2. Określenie wpływu ryzyka polega na określeniu przewidywanych skutków jakie będzie miało, dla realizacji zadania lub osiągnięcia celu w działaniu Urzędu i Jednostek Organizacyjnych, wystąpienie zdarzenia objętego ryzykiem. Do określenia wpływu używany jest opis jakościowy przy zastosowaniu skali ocen: wysoki, średni, niski.
3. Określenie prawdopodobieństwa wystąpienia ryzyka polega na określeniu przewidywanej częstotliwości występowania zdarzenia objętego ryzykiem w trakcie roku. Do określenia prawdopodobieństwa stosowany jest opis jakościowy przy zastosowaniu skali ocen: wysokie, średnie, niskie.
4. Podczas określania wpływu i prawdopodobieństwa ziszczenia się ryzyka stosowane są zasady zawarte w załączniku nr 3 do zarządzenia

§ 7

1. W oparciu o dokonaną ocenę wpływu i prawdopodobieństwa wystąpienia ryzyka ustalany jest poziom istotności ryzyka wskazany w załączniku nr 3 do zarządzenia.
2. Ustala się następujące poziomy istotności ryzyka:
 - a. **ryzyko poważne**, tj. ryzyko o wysokim wpływie oraz wysokim lub średnim prawdopodobieństwie oraz średnim wpływie i wysokim prawdopodobieństwie,
 - b. **ryzyko umiarkowane**, tj. ryzyko o wysokim wpływie i niskim prawdopodobieństwie, ryzyko o średnim wpływie oraz średnim prawdopodobieństwie, a także ryzyko o niskim wpływie i wysokim prawdopodobieństwie;

c. **ryzyko niskie** tj. ryzyko o niskim wpływie oraz średnim lub niskim prawdopodobieństwie.

§ 8

1. Ryzykiem akceptowanym jest ryzyko niskie oraz ryzyko umiarkowane. Ryzyko poważne przekracza akceptowany poziom ryzyka.

2. Ryzyko przekraczające akceptowany poziom ryzyka wymaga ustalenia i podjęcia działań ograniczających je do poziomu umiarkowanego lub niskiego poprzez zmniejszenie jego wpływu lub prawdopodobieństwa ziszczenia się (przeciwdziałanie ryzyku).

§ 9

1. 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;

2. 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.

§ 10

1. Kierownicy komórek organizacyjnych Urzędu oraz kierownicy jednostek organizacyjnych dokonują identyfikacji ryzyka, oceny ryzyka oraz określenia metod przeciwdziałania ryzyku,

na etapie opracowywania propozycji celów i zadań na dany rok budżetowy, wypełniając „Arkusze identyfikacji, oceny oraz określenia metody przeciwdziałaniu ryzyku”, zwane dalej „Arkuszami”, według wzoru zamieszczonego w załączniku nr 4 do zarządzenia.

2. W ramach systemu bezpieczeństwa informacji i danych osobowych, kierownicy komórek organizacyjnych Urzędu, oraz kierownicy jednostek organizacyjnych Miasta identyfikują aktywa organizacji do zagrożeń (utrata poufności, integralności, dostępności, rozliczalności), identyfikują ryzyka oraz wskazują stosowane w komórce organizacyjnej zabezpieczenia techniczne i organizacyjne, a następnie dokonuje szacowania ryzyka, według wzoru stanowiącego załącznik nr 5 do zarządzenia.

3. Arkusze przedkładane są do dnia 31 stycznia każdego roku, celem weryfikacji i akceptacji:

- Audytorowi Wewnętrznemu Urzędu Miasta Sopotu w zakresie zidentyfikowanych ryzyk dotyczących realizacji zadań i celów przez Urząd i Jednostki Organizacyjne,
- Inspektorowi Ochrony Danych w zakresie zidentyfikowanych ryzyk w bezpieczeństwie informacji i danych osobowych.

4. Audytor wewnętrzny i Inspektor Ochrony Danych przekazują Prezydentowi Miasta oraz Sekretarzowi Miasta informację o najistotniejszych ryzykach zagrażających realizacji celów i zadań komórek organizacyjnych Urzędu w formie rejestru ryzyk, stanowiący załącznik nr 6 i nr 7 do zarządzenia.

§ 11

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 w/w 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.

§ 12

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

- 1) kierowników komórek organizacyjnych 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) Prezydenta Miasta, jego Zastępcy w ramach bieżącego zarządzania Urzędem, w tym w szczególności w trakcie narad z kierownikami komórek organizacyjnych 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.

§ 13

Wykonanie zarządzenia powierza się Sekretarzowi Miasta Sopotu.

§ 14

Traci moc Zarządzenie Nr 755/2012 Prezydenta Miasta Sopotu z dnia 02 listopada 2012 r. w sprawie zarządzania ryzykiem w Urzędzie Miasta Sopotu i Jednostkach Organizacyjnych Miasta.

Zarządzenie obowiązuje od dnia podpisania.

PREZYDENT MIASTA

/-/ dr inż. Jacek Karnowski

Załącznik Nr 1

do zarządzenia Nr 1398/2018
Prezydenta Miasta Sopotu
z dnia 4 lipca 2018 roku

Kategorie (obszary) ryzyka

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

Kategorie ryzyka	
Ryzyko finansowe	
Budżetowe	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów
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 2

do zarządzenia Nr 1398/2018
Prezydenta Miasta Sopotu
z dnia 4 lipca 2018 roku

Kategorie (obszary) ryzyka

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

Kategorie ryzyka
Ryzyko naruszenia bezpieczeństwa informacji
Związane z kradzieżą urządzeń, nośników lub dokumentów, ujawnieniem danych, pobieraniem danych z niewiarygodnych źródeł, manipulowaniem urządzeniem oraz sfalszowaniem 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

Ryzyko zniszczenia fizycznego
Związane z pożarem, zalaniem, zniszczeniem urządzeń lub nośników
Ryzyko związane z wystąpieniem zjawiska naturalnego
Związane z wystąpieniem zjawisk pogodowych, sejsmicznych, klimatycznych oraz powodzi

Załącznik Nr 3

do zarządzenia Nr 1398/2018
Prezydenta Miasta Sopotu
z dnia 4 lipca 2018 roku

1. Zasady oceny wpływu ryzyka

Wpływ	Przesłanki
Wysoki (3)	Zdarzenie objęte ryzykiem powoduje uszczerbek mający krytyczny lub bardzo duży wpływ na realizację kluczowych zadań albo osiągnięcie założonych celów – poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa lub na reputacji.
Średni (2)	Zdarzenie objęte ryzykiem powoduje znaczną stratę posiadanych zasobów, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, reputację Urzędu i Jednostek Organizacyjnych. Z wystąpieniem zdarzenia objętego ryzykiem może się wiązać trudny proces przywracania stanu poprzedniego.
Niski (1)	Zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, zakłócenie lub opóźnienie w wykonywaniu zadań. Nie wpływa na reputację Urzędu i Jednostek Organizacyjnych. Skutki zdarzenia można łatwo usunąć.

2 Zasady oceny stopnia prawdopodobieństwa wystąpienia ryzyka

Prawdopodobieństwo	Przesłanki
Wysokie (3)	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku
Średnie (2)	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się kilkakrotnie w ciągu roku
Niskie (1)	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz w ciągu roku lub nie zdarzy się w ciągu roku

3. Poziom istotności ryzyka

Ryzyko poważne (6-9)	Ryzyko o wysokim wpływie oraz wysokim lub średnim prawdopodobieństwie Ryzyko o średnim wpływie i wysokim prawdopodobieństwie
Ryzyko umiarkowane (3-5)	Ryzyko o wysokim wpływie i niskim prawdopodobieństwie, Ryzyko o średnim wpływie oraz średnim lub niskim prawdopodobieństwie Ryzyko o niskim wpływie i wysokim prawdopodobieństwie
Ryzyko nieznaczne (1-2)	Ryzyko o niskim wpływie oraz średnim lub niskim prawdopodobieństwie

Załącznik Nr 4

do zarządzenia Nr 1398/2018

Prezydenta Miasta Sopotu

z dnia 4 lipca 2018 roku

ARKUSZ IDENTYFIKACJI, OCENY ORAZ OKREŚLENIA METODY PRZECIWDZIAŁANIA RYZYKU

Ryzyko						Przeciwdziałanie ryzyku
L.p.	Cel – zadanie	Ryzyko (wskazać występujące kategorie ryzyka)	Wpływ (wskazać jedną z ocen)	Prawdopodobieństwo (wskazać jedną z ocen)	Istotność ryzyka kol.4 x kol.5 (proszę zaznaczyć kolorem czerwonym ryzyka poważne)	Planowana metoda przeciwdziałania ryzyku (działania zaradcze ograniczające ryzyko)
1	2	3	4	5	6	7
1.						
2.						

.....
podpis Kierownika

Zasady wypełniania arkusza:

Nr kolumny	Sposób wypełnienia
1	Numer kolejny celu lub zadania na dany rok pracy Urzędu i Jednostek Organizacyjnych

2	Nazwa celu lub zadania na dany rok pracy Urzędu i Jednostek Organizacyjnych
3	Wskazanie kategorii ryzyka oraz krótki opis jego natury np. ryzyko finansowe-związane z nieterminowym regulowaniem płatności
4	Ocena wpływu w skali : wysoki – średni – niski
5	Ocena prawdopodobieństwa w skali: wysokie – średnie – niskie
6	Poziom istotności ryzyka wynikający z przyznanych ocen prawdopodobieństwa i wpływu : iloczyn kolumn 4 i 5
7	Wskazanie planowanej metody przeciwdziałania ryzyku np. .powierzenie odpowiedzialności wyznaczonemu pracownikowi, bieżący nadzór Skarbnika

Załącznik Nr 5

do zarządzenia Nr 1398/2018

Prezydenta Miasta Sopotu

z dnia 4 lipca 2018 roku

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

Ryzyko						Przeciwdziałanie ryzyku
L.p.	Cel – zadanie	Ryzyko (wskazać występujące kategorie ryzyka)	Wpływ (wskazać jedną z ocen)	Prawdopodobieństwo (wskazać jedną z ocen)	Istotność ryzyka Kol. 4x kol. 5 (proszę zaznaczyć kolorem czerwonym ryzyka poważne)	Planowana metoda przeciwdziałania ryzyku (działania zaradcze ograniczające ryzyko)
1	2	3	4	5	6	7
1.						
2.						

.....
podpis Kierownika

Zasady wypełniania arkusza:

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

Załącznik Nr 6

do zarządzenia Nr 1398/2018

Prezydenta Miasta Sopotu

z dnia 4 lipca 2018 roku

Rejestr ryzyk na rok

L.p.	Obszar ryzyka/ryzyko	Ryzyko*	Właściciel ryzyka (komórka organizacyjna lub osoba)	Reakcja na ryzyko (działania jakie należy podjąć dla ograniczenia/usunięcia ryzyka)
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
1	Obszar działalności np. ochrona środowiska			
2.				
3.				
4.				

*Skala ryzyka: poważne

Rejestr sporządzono na podstawie arkuszy identyfikacji, oceny oraz określenia metod przeciwdziałaniu ryzyku poszczególnych komórek organizacyjnych UM Sopotu.

.....
podpis: Audytora/Inspektora Ochrony Danych

Załącznik Nr 7

do zarządzenia Nr 1398/2018
Prezydenta Miasta Sopotu
z dnia 4 lipca 2018 roku

**Rejestr ryzyk w ramach systemu bezpieczeństwa informacji i danych osobowych
na rok**

L.p.	Obszar ryzyka/ryzyko	Ryzyko*	Właściciel ryzyka (komórka organizacyjna lub osoba)	Reakcja na ryzyko (działania jakie należy podjąć dla ograniczenia/usunięcia ryzyka)
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>
1	Obszar działalności np. ochrona środowiska			
2.				
3.				
4.				

*Skala ryzyka: poważne

Rejestr sporządzono na podstawie arkuszy identyfikacji, oceny oraz określenia metod przeciwdziałaniu ryzyku poszczególnych komórek organizacyjnych UM Sopotu.

.....
podpis: Audytora/Inspektora Ochrony Danych