ZARZĄDZENIE Nr 451/2017

BURMISTRZA SOKÓŁKI

z dnia 29.12.2017r.

w sprawie określenia zasad organizacji i funkcjonowania kontroli zarządczej w gminie Sokółka

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tj. Dz.U. z 2017r. poz. 1875 ze zm. poz. 2232) i art. 69 ust.1 pkt 2 ustawy z dnia 27 sierpnia 2009r., o finansach publicznych (tj. Dz.U. z 2017r. poz. 2077) oraz Komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009r., w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Min. Fin. Nr 15, poz. 84) zarządzam, co następuje:

§ 1

Określa się Regulamin organizacji i funkcjonowania kontroli zarządczej w gminie Sokółka, stanowiący załącznik do niniejszego zarządzenia.

§ 2

Traci moc zarządzenie Nr 43/2011 Burmistrza Sokółki z dnia 29 marca 2011r., w sprawie ustalenia regulaminu kontroli zarządczej w Urzędzie Miejskim w Sokółce i jednostkach organizacyjnych i zasad jej prowadzenia.

§ 3

Wykonanie zarządzenia powierzam Koordynatorowi Kontroli Zarządczej w Urzędzie Miejskim w Sokółce, Zastępcom Burmistrza Sokółki, Skarbnikowi, Kierownikom Wydziałów Urzędu Miejskiego w Sokółce, Dyrektorom jednostek organizacyjnych gminy.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Ewa Kulikowska

28.12.2017 r.
RADCA PRAWNY
mgr Urszula Moniuszko
BŁ - 740

28.12.2017

Iwona Aleksza
Audytor wewnętrzny
28.12.2017

Załącznik Nr 1
do Zarządzenia Nr 451/2017
Burmistrza Sokółki
z dnia 29.12.2017

REGULAMIN
ORGANIZACJI I FUNKCJONOWANIA KONTROLI ZARZĄDCZEJ
W GMINIE SOKÓŁKA

Rozdział I
POSTANOWIENIA OGÓLNE

§ 1

Regulamin organizacji i funkcjonowania kontroli zarządczej w Gminie Sokółka określa:
1/ organizację kontroli zarządczej, w tym system jej koordynacji,
2/ zasady wykonywania kontroli zarządczej w Urzędzie Miejskim w Sokółce oraz obowiązki jednostek organizacyjnych w tym zakresie.

§ 2

Ilekroć w regulaminie organizacji i funkcjonowania kontroli zarządczej w Gminie Sokółka jest mowa o:
1/ Gminie- należy przez to rozumieć gminę w rozumieniu przepisów o samorządzie gminnym,
2/ Burmistrzu – należy przez to rozumieć Burmistrza Sokółki,
3/ Zastępców Burmistrza - należy przez to rozumieć I Zastępcę Burmistrza Sokółki i II Zastępcę Burmistrza Sokółki,
4/ Sekretarzu – należy przez to rozumieć Sekretarza Sokółki,
5/ Skarbniku – należy przez to rozumieć Skarbnika Sokółki,
6/ Kierowniku – należy przez to rozumieć Kierowników danego Wydziału Urzędu Miejskiego w Sokółce,
7/ Urzędzie – należy przez to rozumieć Urząd Miejski w Sokółce,
8/ Regulaminie – należy przez to rozumieć Regulamin organizacji i funkcjonowania kontroli zarządczej w Gminie Sokółka,
9/ Jednostce organizacyjnej gminy – należy przez to rozumieć gminną jednostkę organizacyjną utworzoną w celu realizacji zadań Gminy Sokółka
10/ Dyrektorze jednostki – należy przez to rozumieć Dyrektora gminnej jednostki organizacyjnej,
11/ Zarządzeniu - należy przez to rozumieć Zarządzenie Burmistrza Sokółki Nr ..... z dnia ..... w sprawie określenia organizacji i funkcjonowania kontroli zarządczej w Gminie Sokółka.

§ 3

Kontrola zarządcza stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

§ 4

Kontrola zarządcza funkcjonuje na dwóch poziomach:
1/ I poziom, czyli kontrola zarządcza pierwszego stopnia – stanowi ją kontrola sprawowana przez Burmistrza, a realizowana za pośrednictwem kierowników wydziałów i dyrektorów jednostek organizacyjnych Gminy.
2/ II poziom, czyli kontrola zarządcza realizowana na poziomie Gminy, za prowadzenie której odpowiedzialny jest Burmistrz.

§ 5

Celem kontroli zarządczej jest:
1/ Podejmowanie działań we wszystkich aspektach funkcjonowania Urzędu zgodnie z przepisami prawa oraz procedurami wewnętrznymi,
2/ Skuteczne i efektywne działanie,
3/ Sporządzanie wiarygodnych sprawozdań,
4/ Ochrona zasobów,
5/ Przestrzeganie i promowanie zasad etycznego działania,
6/ Efektywny i skuteczny system przepływu informacji,
7/ Zarządzanie ryzykiem .

§ 6

1/ Misją Urzędu Miejskiego w Sokółce jest sprawny i skuteczny urząd, realizujący efektywnie we współpracy z innymi partnerami określone prawem zadania i usługi na rzecz rozwoju Gminy i jego społeczności.
2/ Nadrzędnym celem Urzędu Miejskiego w Sokółce jest świadczenie usług najwyższej jakości, spełniających potrzeby i oczekiwania społeczności lokalnej oraz innych naszych Klientów, na podstawie i w granicach obowiązującego prawa oraz wspieranie rozwoju społeczno – gospodarczego Gminy i jego skuteczne zarządzanie. Przyjmując ten priorytet, działamy na rzecz stałego podnoszenia jakości obsługi Klientów oraz tworzenia profesjonalnej administracji samorządowej. Uznając za niezbędne i celowe wdrażanie nowoczesnych metod zarządzania doskonalimy przyjęty system organizacyjny opierając się na sprawdzonych standardach zarządzania.
3/ Do obowiązków pracowników Urzędu należy aktywny udział w realizowanym procesie kontroli zarządczej.

ROZDZIAŁ II

FUNKCJONOWANIE STANDARDÓW KONTROLI ZARZĄDCZEJ W URZĘDZIE MIEJSKIM W SOKÓŁCE

§ 7

Sprawowanie kontroli zarządczej w Urzędzie Miejskim w Sokółce zawarte jest w pięciu obszarach standardów i odpowiada poszczególnym elementom kontroli zarządczej:
1/ Środowisko wewnętrzne,
2/ Cele i zarządzanie ryzykiem,
3/ Mechanizmy kontroli,
4/ Informacja i komunikacja,
5/ Monitorowanie i ocena.

§ 8

Aby spełnić wymagania odnoszące się do sprawowania kontroli zarządczej w Urzędzie Miejskim w Sokółce podejmuje się następujące działania:
1/ Przestrzeganie wartości etycznych:
a/ Osoby zarządzające oraz pracownicy Urzędu Miejskiego w Sokółce powinni znać i przestrzegać zasady określone w Kodeksie Etyki Pracowników Urzędu Miejskiego w Sokółce,
b/ Osoby zarządzające powinny wspierać i promować przestrzeganie wartości etycznych dając dobry przykład codziennym postępowaniem i podejmowanymi decyzjami,
c/ Naruszenie przez pracownika Urzędu Miejskiego w Sokółce postanowień Kodeksu Etyki powoduje odpowiedzialność regulaminową (porządkową) oraz przewidziane prawem konsekwencje, a także znajduje odzwierciedlenie w okresowej ocenie dokonywanej zgodnie z obowiązującą w Urzędzie Miejskim w Sokółce procedurą.

2/ Kompetencje zawodowe:
a/ Osoby zarządzające i pracownicy powinni posiadać odpowiednie kwalifikacje i wiedzę. W związku z tym proces zatrudnienia należy prowadzić w sposób zapewniający wybór najlepszego kandydata na dane stanowisko pracy zgodnie z zasadami określonymi w procedurze naboru pracowników,
b/ Kompleksowej ocenie wyników pracy pracowników, pod kątem realizacji wytyczonych celów, określenia przydatności zawodowej na danym stanowisku oraz możliwości rozwojowych pracownika, dokonuje się na podstawie procedury „Okresowych ocen kwalifikacyjnych pracowników samorządowych". Celem okresowych ocen jest także ułatwienie planowania rozwoju pracownika, podejmowania decyzji w zakresie przeszeregowań pracowników, tworzenia kadry rezerwowej, usprawnienia funkcjonowania systemu motywującego,
c/ Burmistrz zapewnia rozwój kompetencji zawodowych pracowników jednostki oraz osób zarządzających poprzez system szkoleń i samokształcenia.

3/ Struktura organizacyjna:
a/ Zakres zadań poszczególnych komórek organizacyjnych jednostki oraz zakres podległości określa Regulamin Organizacyjny Urzędu Miejskiego w Sokółce,
b/ Każdemu pracownikowi zatrudnionemu w Urzędzie powierza się zakres zadań określony w pisemnym, indywidualnym zakresie obowiązków, uprawnień i odpowiedzialności, który sporządza bezpośredni przełożony, a zatwierdza Burmistrz,
c/ W Urzędzie Miejskim w Sokółce obowiązuje Regulamin Pracy, ustalający organizację i porządek w procesie pracy oraz związane z tym prawa i obowiązki pracodawcy i pracowników.

4/ Delegowanie uprawnień:
a/ Zakres uprawnień osób zarządzających i pracowników określa indywidualny zakres czynności, natomiast w odniesieniu do gospodarki finansowej jest precyzyjnie określony w udzielonych na piśmie imiennych upoważnieniach.

§ 9

W ramach określenia celów działalności i zarządzania ryzykiem, sposób hierarchizacji ustalania celów, zadań, zasady związane z zarządzaniem ryzykiem określa szczegółowo rozdział VIII niniejszego regulaminu.

§ 10

W ramach mechanizmów kontroli, zorganizowano w Urzędzie Miejskim w Sokółce system kontroli zarządczej oparty na poniższych rodzajach kontroli:

1/ kontroli instytucjonalnej realizowanej przez podmioty zewnętrzne, a w szczególności przez Regionalną Izbę Obrachunkową, Najwyższą Izbę Kontroli, Urząd Kontroli Skarbowej, Zakład Ubezpieczeń Społecznych oraz inne organy i instytucje prowadzące działalność w zakresie kontroli i nadzoru,
2/ audytu wewnętrznego, w szczególności w zakresie oceny procesu zarządzania ryzykiem oraz realizacji zadań zapewniających i czynności doradczych,
3/ kontroli finansowej, sprawowanej przez Skarbnika oraz głównych księgowych w jednostkach organizacyjnych gminy,
4/ kontroli funkcjonalnej, sprawowanej przez osoby zajmujące stanowiska kierownicze w Urzędzie i jednostkach organizacyjnych oraz osób wyznaczonych do realizacji powierzonych zadań,
5/ kontroli wewnętrznej i zewnętrznej sprawowanej przez jednostki organizacyjne gminy zgodnie z zadaniami powierzonymi w Regulaminie Organizacyjnym Urzędu oraz inne upoważnione do tego osoby,
6/ samokontroli pracowniczej.

§ 11

Do obowiązków pracowników Urzędu należy aktywny udział w realizowanym procesie kontroli zarządczej.

ROZDZIAŁ III
KOORDYNACJA KONTROLI ZARZĄDCZEJ W URZĘDZIE MIEJSKIM W SOKÓŁCE

§ 12

1/ Koordynację kontroli zarządczej w Urzędzie prowadzi Koordynator kontroli zarządczej.
2/ Zadaniem Koordynatora jest prowadzenie bieżącej analizy informacji zarządczych pochodzących ze źródeł, o których mowa w § 5 Regulaminu, wskazujących na występujące zagrożenia w osiągnięciu celów lub zadań oraz inicjowanie działań: korekcyjnych, korygujących, naprawczych, bądź wspomagających.
3/ Nadzór merytoryczny nad opracowaniem planów, programów, sprawozdań oraz kwestiami związanymi z zarządzaniem ryzykiem w wydziałach urzędu sprawują właściwi Kierownicy Urzędu Miejskiego w Sokółce.

ROZDZIAŁ IV
PODSTAWOWE FUNKCJE I ZASADY KONTROLI ZARZĄDCZEJ W URZĘDZIE MIEJSKIM W SOKÓŁCE

§ 13

1/ Kontrola zarządcza to ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy, obejmujących następujące obszary:
a/ zgodność działań z przepisami prawa oraz procedurami wewnętrznymi,
b/ skuteczności i efektywności działania,
c/ wiarygodności sprawozdań,
d/ ochrony zasobów oraz stosowanie fizycznych środków kontroli nad majątkiem,
e/ przestrzegania i promowania zasad etycznego postępowania,
f/ efektywności i skuteczności przepływu informacji
g/ zarządzania ryzykiem,
h/ monitoringu działań.
2/ System kontroli zarządczej w Urzędzie to zbiór elementów zarządczych i czynności kontrolnych obejmujących w szczególności:
a/ samokontrolę,
b/ kontrolę funkcjonalną,
c/ kontrolę instytucjonalną.
3. Do samokontroli zobowiązani są wszyscy pracownicy zatrudnieni w Urzędzie bez względu na stanowisko i rodzaj wykonywanej pracy.
a/ samokontrola, polega na kontroli prawidłowości własnej pracy w oparciu o obowiązujące przepisy prawa i obowiązki wynikające z posiadanego zakresu czynności służbowych,
b/ w przypadku ujawnienia nieprawidłowości pracownik dokonujący samokontroli jest zobowiązany:
- podjąć niezbędne działania zmierzające do ich usunięcia,
- niezwłocznie poinformować o nich przełożonego
c/ Kierownik wydziału lub dyrektor jednostki organizacyjnej Gminy, który został poinformowany o ujawnionych nieprawidłowościach zobowiązany jest niezwłocznie podjąć decyzję w sprawie dalszego toku postępowania w odniesieniu do ujawnionych nieprawidłowości.
4. Kontrola funkcjonalna sprawowana jest przez Kierowników wydziałów, dyrektorów jednostek organizacyjnych Gminy oraz inne osoby biorące udział w realizacji określonych zadań, operacji, procesów, których obowiązki wykonywania kontroli funkcjonalnej zostały określone w zakresach czynności, bądź którzy do wykonywania tej kontroli zostali zobligowani na podstawie innych przepisów.
5. Istotą wspólną czynności kontrolnych jest szczegółowe zbadanie stanu faktycznego i porównanie go z obowiązującą dla niego normą oraz ustalenie odchyleń od tej normy.

§ 14

Kontrola zarządcza powinna być:

1/ adekwatna – co oznacza, że jest zgodna z zasadami określonymi w obowiązujących aktach prawnych oraz z Regulaminem, dokładnie odpowiadająca założonym celom kontroli zarządczej. Zasady kontroli powinny być tak skonstruowane, żeby ich prawidłowe stosowanie zabezpieczyło Urząd i gminne jednostki organizacyjne przed danym ryzykiem,

2/ skuteczna – co oznacza, że jest tak skonstruowana, aby faktycznie zabezpieczyła Urząd i gminne jednostki organizacyjne przed wystąpieniem lub skutkami danego ryzyka,

3/ efektywna – co oznacz, że powinna powodować osiąganie założonych celów. Kontrola zarządcza powinna ograniczać ryzyko w pożądanym stopniu przy wykorzystaniu najmniejszych możliwych nakładów.

§ 15

Podstawowe funkcje kontroli zarządczej to:

1/ monitorowanie stopnia realizacji celów i zadań z przyjętymi założeniami oraz w przypadku gdy jest to konieczne, podejmowanie działań korygujących,

2/ uzyskanie racjonalnego zapewnienia, że wydatki publiczne są dokonywane:

a/ w sposób celowy i oszczędny z zachowaniem zasad uzyskiwania najlepszych efektów z danych nakładów oraz optymalnego doboru metod i środków służących osiągnięciu założonych celów,

b/ w sposób umożliwiający terminową realizację zadań,

c/ w wysokości i terminach wynikających z wcześniej zaciągniętych zobowiązań,

d/ zgodnie z przepisami prawa,

3/ ocena prawidłowości realizowanych zadań.

Rozdział V

PODSTAWOWE MECHANIZMY KONTROLI STOSOWANE W URZĘDZIE MIEJSKIM W SOKÓŁCE

§ 16

Wśród podstawowych mechanizmów kontroli stosowanych w Urzędzie Miejskim w Sokółce wymienić należy:

1/ Dokumentowanie systemu kontroli zarządczej – w ramach tego systemu działają procedury wewnętrzne, regulaminy, instrukcje, wytyczne, dokumenty określające zakres obowiązków, uprawnień i odpowiedzialności pracowników oraz inne wewnętrzne dokumenty,

2/ Nadzór nad realizacją zadań – zakres nadzoru wynika z Regulaminu Organizacyjnego Urzędu Miejskiego w Sokółce, zwłaszcza w częściach dotyczących zasad kierowania pracą Urzędu, podziału zadań pomiędzy stanowiskami kierowniczymi oraz zakresu działania poszczególnych komórek organizacyjnych, a także wynika z indywidualnych zakresów czynności,

3/ Ciągłość działalności – mechanizm służący utrzymaniu ciągłości działalności, polega min. na wyznaczaniu osób pełniących zastępstwo podczas nieobecności kluczowych osób odpowiedzialnych za zarządzanie w Urzędzie (w formie stosownych upoważnień oraz odpowiedniego zapisu w zakresach obowiązków).

4/ Ochrona zasobów – dostęp do zasobów finansowych, materialnych i informacyjnych jednostki mają wyłącznie upoważnione osoby. Wprowadzono stosowne ograniczenia w dostępie do newralgicznych miejsc takich jak serwerownia, kancelaria tajna, archiwum. Budynek Urzędu wyposażony jest w systemy alarmowe i monitorujące. Budynek urzędu wyposażony jest w podstawowy sprzęt przeciwpożarowy.

Powierza się pracownikom odpowiedzialność materialną za przekazane składniki majątkowe.

Stan mienia jednostki jest systematycznie weryfikowany i porównywalny ze stanem ewidencyjnym w drodze inwentaryzacji na podstawie Instrukcji inwentaryzacyjnej.

Ochrony dokumentacji dokonuje się na zasadach określonych w Instrukcji kancelaryjnej i Polityce bezpieczeństwa.

5/ Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych – szczegółowo opisane zostały w Instrukcji obiegu dokumentów finansowo – księgowych w Urzędzie Miejskim w Sokółce.
Podział kluczowych obowiązków wynika z Regulaminu Organizacyjnego Urzędu Miejskiego w Sokółce, indywidualnych zakresów czynności oraz wydanych upoważnień.
6/ Mechanizmy kontroli dotyczące systemów informatycznych – w Urzędzie funkcjonują mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych, szczegółowo opisanych w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym.

Rozdział VI

ODPOWIEDZIALNOŚĆ KIEROWNIKÓW JEDNOSTEK URZĘDU I DYREKTORÓW GMINNYCH JEDNOSTEK ORGANIZACYJNYCH

§ 17

Kierownicy wydziałów Urzędu Miejskiego oraz Dyrektorzy gminnych jednostek organizacyjnych ponoszą odpowiedzialność za nadzorowanie i kontrolowanie procesów zachodzących w kierowanych przez nich jednostkach w sposób dający Burmistrzowi rozsądne zapewnienie, że:
1/ działania podległych ich jednostek pozostają w zgodzie z przepisami prawa i zasadami (procedurami) przyjętymi w jednostce oraz ze standardami,
2/ zasoby są zużywane oszczędnie, w sposób przynoszący pożytek, a usługi świadczone są na odpowiednim poziomie,
3/ zadania są realizowane efektywnie i skutecznie, plany jednostek, programy, zamierzenia i cele są osiągane,
4/ dane i informacje są publikowane lub udostępniane wewnętrznie, czy na zewnątrz rzetelne, wiarygodne i aktualne,
5/ zasady, a w szczególności składniki majątku, w tym dane osobowe i informacje niejawne są zabezpieczone przez zniszczeniem, utratą i defraudacją,
6/ ryzyka związane z realizacją zadań są na bieżąco identyfikowane i monitorowane celem ciągłej poprawy procesów.
7/ zasady etycznego postępowania są przestrzegane i promowane.

Rozdział VII

OBOWIĄZKI KIEROWNIKÓW WYDZIAŁU URZĘDU I DYREKTORÓW GMINNYCH JEDNOSTEK ORGANIZACYJNYCH

§ 18

1/ Do obowiązków poszczególnych Kierowników wydziałów i Dyrektorów gminnych jednostek organizacyjnych w zakresie ustanowienia i sprawowania kontroli zarządczej należy:
a/ utworzenie planów działań, wyznaczenie celów i zadań dla wydziałów Urzędu i jednostek organizacyjnych gminy, a także monitorowania realizacji wyznaczonych celów i zadań,
b/ wprowadzenie systemów oraz procedur zarządzania ryzykiem opartych na sformułowanych celach i zadaniach. Zarządzanie ryzykiem obejmuje następujące czynności:
- identyfikowanie ryzyka dla poszczególnych obszarów,
- analiza i ocena zagrożeń,
- reakcja na ryzyko tj. podejmowanie decyzji i działań korygujących (lub dla rozwiązania problemów),
- monitorowanie występowania zagrożeń (stanów niepożądanych),
- okresowa aktualizacja ryzyka i zagrożeń
c/ przekazywanie w formie sprawozdań informacji o stopniu realizacji zadań. W przypadku braku bądź nieterminowej realizacji celów i zadań sprawozdanie powinno wskazać przyczyny zaistniałego stanu,
d/ składanie przez dyrektorów gminnych jednostek organizacyjnych oświadczeń o stanie kontroli zarządczej w jednostkach przez nich kierowanych,

e/ zapewnienie skuteczności wykonywania kontroli zarządczej i dbałość o ciągłą poprawę realizowanych przez siebie procesów.
2/ Poszczególne wydziały Urzędu sporządzają plany działań, na każdy kolejny rok, według wzoru stanowiącego Załącznik Nr 2 Zarządzenia Burmistrza. W planach działań określa się cele oraz zadania, które będą podstawą do realizowania tych celów oraz zasad ich monitorowania.
3/ Kierownicy poszczególnych wydziałów Urzędu, przedstawiają je Burmistrzowi do zatwierdzenia w terminie do dnia 15 grudnia każdego roku.

Rozdział VIII
ZARZĄDZANIE RYZYKIEM

§ 19

1/ Kierownicy wydziałów Urzędu Miejskiego w Sokółce i Dyrektorzy gminnych jednostek organizacyjnych, biorąc pod uwagę cele kontroli zarządczej oraz przypisany w tym obszarze zakres odpowiedzialności, organizują w podległych im jednostkach adekwatną, skuteczną i efektywną kontrolę zarządczą , uwzględniając standardy kontroli zarządczej.
2/ Dla realizacji obowiązków zapisanych w § 18 Regulaminu, Kierownicy wydziałów i Dyrektorzy jednostek organizacyjnych gminy przygotowują i wdrażają procedury zarządzania ryzykiem.
3/ System zarządzania ryzykiem w jednostkach opiera się na sformalizowanych w ramach procedury budżetowej mierzalnych celach i zadaniach.
4/ Ryzyko odnosi się do celów, polityk i programów, a w szczególności do tych określonych w § 18 ust. 2

Rozdział IX
AUDYT WEWNĘTRZNY

§ 20

1/ Audyt wewnętrzny prowadzony w Urzędzie i gminnych jednostkach organizacyjnych jest działalnością niezależną i obiektywną, której celem jest wspieranie Burmistrza w realizacji celów i zadań poprzez systematyczną ocenę kontroli zarządczej oraz czynności doradcze.
2/ Celem pracy audytu wewnętrznego, jest ustalenie, czy wprowadzony przez kierownictwo system zarządzania ryzykiem, system kontroli zarządczej i ład organizacyjny są odpowiednie i czy funkcjonują w sposób zapewniający wykonanie standardów.
3/ Audyt wewnętrzny dokonuje oceny adekwatności, skuteczności i efektywności systemu kontroli zarządczej na podstawie przeprowadzonych zadań audytowych i w razie stwierdzenia konieczności podjęcia określonych działań przedstawia rekomendację w kierunku poprawy tego systemu.
4/ Zasady i tryb przeprowadzenia audytu określają odrębne przepisy.

Rozdział X
OŚWIADCZENIE O STANIE KONTROLI ZARZĄDCZEJ

§ 21

1/ Oświadczenie o stanie kontroli zarządczej (z zastrzeżeniem albo bez zastrzeżeń), podpisuje Dyrektor jednostki organizacyjnej w oparciu o fakty i zdarzenia, które miały miejsce w jednostce. Wzór oświadczenia stanowi Załącznik Nr 3 do Zarządzenia Burmistrza.
2/ Oświadczenie o stanie kontroli zarządczej Dyrektorzy jednostek organizacyjnych gminy przekazują do Urzędu Miejskiego w terminie do 31 stycznia danego roku kalendarzowego.
3/ Koordynator kontroli zarządczej w Urzędzie Miejskim w Sokółce na podstawie informacji uzyskanych od jednostek organizacyjnych, wyników kontroli podmiotów zewnętrznych oraz zadań przeprowadzonych przez upoważnionych pracowników, sporządza sprawozdanie o stanie kontroli zarządczej.

Rozdział XI

SAMOOCENA

§ 22

1/ Samoocena umożliwia Kierownikowi jednostki dokonanie przeglądu istniejących mechanizmów kontroli pod względem adekwatności oraz wdrażania ulepszeń.

2/ Kierownicy wydziałów Urzędu Miejskiego w Sokółce raz w roku przeprowadzają samoocenę kontroli zarządczej oraz sporządzają z niej informację, według wzoru stanowiącego Załącznik Nr 4 do Zarządzenia Burmistrza.

3/ Proces samooceny powinien być udokumentowany.

4/ Koordynator kontroli zarządczej w Urzędzie przedkłada Burmistrzowi Sokółki, nie później niż do ostatniego dnia lutego informację na temat stanu kontroli zarządczej w Urzędzie oraz propozycję usprawnień, w przypadku braku realizacji standardów kontroli zarządczej, wraz ze sprawozdaniem, o którym mowa w § 21 ust.3

Rozdział XII

MONITOROWANIE I OCENA

§ 23

1/ Ocena systemu kontroli zarządczej, w tym systemu zarządzania ryzykiem, w Urzędzie i w jednostkach organizacyjnych gminy powinna być prowadzona w sposób ciągły.

2/ Zidentyfikowane ryzyko oraz ustalone metody jego ograniczania są na bieżąco oceniane przez Kierowników Wydziału Urzędu i Dyrektorów jednostek organizacyjnych gminy, którzy oceniają poziom zidentyfikowanego ryzyka oraz skuteczność stosowanych metod jego ograniczenia.

3/ Wyniki oceny, o której mowa w pkt 2 wykorzystywane są na bieżąco do poprawy efektywności zarządzania ryzykiem wewnętrznym oraz usprawnienia systemu kontroli zarządczej.

4/ Kierownicy Wydziałów Urzędu Miejskiego w Sokółce, w terminie do dnia 15 lutego każdego roku składają informację za rok poprzedni, według wzorów stanowiących Załączniki Nr 5 i 6 do Zarządzenia Burmistrza, dotyczą realizacji planu działania oraz ryzyka zidentyfikowanego w roku poprzednim, zawierającą w szczególności ocenę skuteczności zaproponowanych (przyjętych) metod przeciwdziałania ryzyku oraz wpływu tych metod na poziom istotności ryzyka do Koordynatora kontroli zarządczej.

5/ Dyrektorzy jednostek organizacyjnych gminy składają wyłącznie oświadczenie o stanie kontroli zarządczej, zgodnie z postanowieniami Zarządzenia Burmistrza, określającego zasady sprawowania kontroli zarządczej w Gminie Sokółka.

Rozdział XIII

MECHANIZMY KONTROLNE

§ 24

1/ Zadaniem mechanizmów kontroli jest zapobieganie urzeczywistnieniu się ryzyka (lub ograniczenie strat). Każdy zastosowany mechanizm kontrolny, powinien stanowić odpowiedź na konkretne ryzyko. Koszt wdrożenia mechanizmów kontroli nie może być wyższy niż uzyskane dzięki nim korzyści.

2/ Do ogólnych mechanizmów kontroli należy:

a/ dokumentowanie systemu kontroli zarządczej (procedury, instrukcje, zarządzenia, zakresy czynności, regulamin organizacyjny)

b/ dokumentowanie i rejestrowanie operacji finansowych i gospodarczych,

c/ nadzór,

d/ ciągłość działalności,

e/ ochrona zasobów,

f/ mechanizmy kontroli dotyczące systemów informatycznych,

g/ kontrola wewnętrzna (funkcjonalna i instytucjonalna).

3/ W związku z dostosowaniem systemu zarządzania bezpieczeństwem informacji w Urzędzie Miejskim w Sokółce , przyjmuje się do realizacji zadania niezbędne dla zachowania zgodności systemu z wymogami prawnymi (ustawa z dnia 29.08.1997 o ochronie danych osobowych), których zbiór określa Załącznik Nr 7 do niniejszego Zarządzenia.

BURMISTRZ

Ewa Kulikowska

Załącznik Nr 2
do Zarządzenia Nr 451/2017
Burmistrza Sokółki
z dnia 29.12.2017

Plany działań, główne cele i zadania
Wydziałów Urzędu Miejskiego w Sokółce na rok .....

Lp.	Cel/Zadanie	Termin realizacji	Miernik osiągnięcia celu	Osoba odpowiedzialna	Uwagi
1	2	3	4	5	6

.....
Akceptacja Zastępcy Burmistrza/Sekretarza/Skarbnika/
Sprawującego nadzór nad Wydziałem

.....
Data i podpis Burmistrza Sokółki

BURMISTRZ
Ewa Kulikowska

Załącznik Nr 3
do Zarządzenia Nr 451/2017
Burmistrza Sokółki
z dnia 29.12.2017

Oświadczenie o stanie kontroli zarządczej za rok .....

Jako osoba odpowiedzialna za zapewnienie i funkcjonowanie adekwatnej, skutecznej i efektywnej kontroli zarządczej, tj. działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny w prawem, efektywny, oszczędny i terminowy, a w szczególności dla zapewnienia:
- zgodności działalności z przepisami prawa i procedurami wewnętrznymi,
- skuteczności i efektywności działania,
- wiarygodności sprawozdań,
- ochrony zasobów,
- przestrzegania i promowania zasad etycznego postępowania,
- efektywności i skuteczności przepływu informacji,
- zarządzania ryzykiem,

Oświadczam, że w kierowanej przez mnie jednostce sektora finansów publicznych
.....
(nazwa jednostki sektora finansów publicznych)

☐1. w wystarczającym stopniu funkcjonowała adekwatna, skuteczna i efektowna kontrola zarządcza.

☐2. w ograniczonym stopniu funkcjonowała adekwatna, skuteczna i efektowna kontrola zarządcza

1/ Zastrzeżenia dotyczą:
.....
.....
.....

2/ Zostaną podjęte następujące działania w celu poprawy funkcjonowania kontroli zarządczej:
.....
.....
.....
.....

☐3/ Nie funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.

a/ Zastrzeżenia dotyczą:
.....
.....
.....
.....

b/ Zostaną podjęte następujące działania w celu poprawy funkcjonowania kontroli zarządczej:.....
.....
.....
.....

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

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

d/ Niniejsze oświadczenie opiera się na mojej ocenie i informacjach dostępnych w czasie sporządzania niniejszego oświadczenia pochodzących z:
- monitoringu realizacji celów i zadań,
- samooceny kontroli zarządczej przeprowadzonej z uwzględnieniem standardów kontroli zarządczej dla sektora finansów publicznych,
- systemu zarządzania ryzkiem,
- audytu wewnętrznego,
- kontroli wewnętrznych,
- kontroli zewnętrznych,
- innych źródeł

informacji:.....
.....

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

.....
(miejscowość, data)

.....
(Dyrektor jednostki)

BURMISTRZ

Ewa Kulikowska

Załącznik Nr 4
do Zarządzenia Nr 451/2017
Burmistrza Sokółki
z dnia 29.12.2017

Samoocena systemu kontroli zarządczej
w
Wydziale Urzędu Miejskiego w Sokółce.....

Lp.		TAK	NIE	Uwagi
1.	Działania podległego mi wydziału pozostają w zgodzie w przepisami prawa i zasadami (procedurami) przyjętymi w jednostce oraz ze standardami			
2.	Zasoby są zużywane oszczędnie i w sposób przynoszący pożytek, a usługi świadczone są na odpowiednim poziomie			
3.	Zadania są realizowane efektywnie i skutecznie, plany jednostek, programy, zamierzenia i cele osiągane			
4.	Dane i informacje publikowane lub udostępniane wewnętrznie, czy na zewnątrz są rzetelne, wiarygodne i aktualne			
5.	Zasoby a w szczególności składniki majątku, w tym dane osobowe i informacje niejawne są zabezpieczone przed zniszczeniem, utratą i defraudacją			
6.	Ryzyko związane z realizacją zadań są na bieżąco identyfikowane i monitorowane celem ciągłej poprawy procesów			
7.	Zasady etycznego postępowania są przestrzegane i promowane			

.....
/Akceptacja Zastępcy Burmistrza/Sekretarza/Skarbnika/
sprawującego nadzór nad Wydziałem/

.....
Podpis Burmistrza Sokółki

BURMISTRZ
Ewa Kulikowska

Załącznik Nr 5
do Zarządzenia Nr 451/2017
Burmistrza Sokółki
z dnia 29.12.2017

Informacja dotycząca realizacji planu działania na rok .....

Lp.	Cel/Zadanie	Termin realizacji	Czy cel/zadanie zostało zrealizowane (tak/nie/ w jakim stopniu)	Sposób realizacji zadania lub przyczyni	Uwagi
1	2	3	4	5	
1.					
2.					

.....
/Akceptacja Zastępcy Burmistrza/Sekretarza/Skarbnika sprawującego nadzór nad Wydziałem/

.....
Podpis Burmistrza Sokółki

BURMISTRZ

Ewa Kulikowska

Załącznik Nr 6
do Zarządzenia Nr 451/2017
Burmistrza Sokółki
z dnia 29.12.2017

Informacja dotycząca ryzyka zidentyfikowanego podczas realizacji zadań w roku.....

Lp.	Cel/Zadanie	Zidentyfikowane ryzyko	Czy ryzyko wystąpiło (tak/nie)	Skutki wystąpienia ryzyka	Działania podjęte	Uwagi
1	2	3	4	5	6	7
1.						
2.						

.....
/Akceptacja Zastępcy Burmistrza/Sekretarza/Skarbnika sprawującego nadzór nad Wydziałem/

.....
Podpis Burmistrza Sokółki

BURMISTRZ
Ewa Kulikowska

Załącznik Nr 7
do Zarządzenia Nr 451/2017
Burmistrza Sokółki
z dnia 29.12.2017

PROCEDURY ZARZĄDZANIA RYZYKIEM INFORMATYCZNYM

W URZĘDZIE MIEJSKIM W SOKÓŁCE

1. WSTĘP

W związku z dostosowaniem systemu zarządzania bezpieczeństwem informacji w Urzędzie Miejskim w Sokółce , przyjmuje się do realizacji zadania niezbędne dla zachowania zgodności systemu z wymogami prawnymi (ustawa z dnia 29.08.1997 o ochronie danych osobowych)

Jedną z kluczowych elementów systemu zarządzania bezpieczeństwem informacji jest analiza i oszacowanie ryzyka związanego z istniejącymi lub potencjalnymi zagrożeniami dla zasobów i aktywów informacyjnych funkcjonujących w jednostce oraz naruszenia ciągłości działania jednostki. Działania te są dokumentowane w postaci metodyki zarządzania ryzykiem, zawierającym definicje kryteriów klasyfikacji informacji, definicję kryteriów ryzyk akceptowanych i nieakceptowalnych, raportu z analizy ryzyka, planu postępowania z ryzykiem.

2. TERMINOLOGIA

Aktyw informacyjny – wszystko co ma wartość dla jednostki oraz stanowi istotny element przetwarzania informacji,
Dostępność – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu w celu zrealizowania określonego zadania ,
Zasób informacyjny – nieformalny zbiór informacji podobnych pod kątem zawartości informacyjnej i jej wartości dla jednostki,
Integralność – właściwość zapewnienia dokładności i kompletności w celu zrealizowania określonego zadania,
Klasyfikacja informacji – dokument systemowy dokonujący klasyfikacji występujących w organizacji informacji, aktywów i zasobów informacyjnych, odzwierciedlający potrzeby priorytety oraz oczekiwany poziom ochrony przy ich przetwarzaniu,
Ustalenie kontekstu – definiowanie, zewnętrznych i wewnętrznych parametrów, które powinny być uwzględniane podczas zarządzania ryzykiem, jak również podczas określania zakresu, kryteriów ryzyka dla polityki zarządzania ryzkiem,
Podatność – cecha zasobu powodująca, że zasób jest narażony na działanie jednego lub wielu zagrożeń,
Punkt krytyczny – potencjalny negatywny czynnik poddawany ocenie będący podstawą do wyznaczenia ryzyka (zagrożenie lub podatność) Punkt krytyczny scharakteryzowany jest następującymi atrybutami:
- prawdopodobieństwo realizacji punktu krytycznego,
- skutek realizacji punktu krytycznego,
- wykrywalność.
Zabezpieczenie – rozwiązanie techniczne lub organizacyjne minimalizujące ryzyko,
Zagrożenie – niepożądane działanie lub sytuacja dotycząca aktywu lub grupy aktywów, która może niekorzystnie wpłynąć na prawidłowość oraz bezpieczeństwo procesów realizowanych w organizacji

3. IDEA METODY ZARZĄDZANIA RYZYKIEM

3.1 ZAŁOŻENIA

Skuteczne zarządzanie ryzykiem w obszarze bezpieczeństwa informacji wymaga od przyjętej metody liczenia ryzyka spełnienia następujących warunków:
- zapewnienia powtarzalności i porównywalności wyników,
- uwzględnienia stopnia wrażliwości informacji,
- uwzględnienia prawdopodobieństwa wystąpienia zdarzenia (zagrożenia) i konsekwencji jego realizacji (skutków)
- uwzględnienia efektywności funkcjonujących zabezpieczeń, wpływających na prawdopodobieństwo zajścia zdarzeń, jak i na późniejsze ewentualne konsekwencje ich realizacji.

3.2 PODSTAWY PROPONOWANEJ METODY OSZACOWANIA RYZYKA

Najważniejszymi elementami metody szacowania ryzyka są: ustalenie kontekstu działalności jednostki oraz klasyfikację posiadanych zasobów informatycznych. Kontekst działalności jest to zestaw czynników wewnętrznych i zewnętrznych, które stanowią o istnieniu urzędu, jego celach oraz sposobach ich realizacji, oczekiwaniach jakie ma spełnić. Kontekst działalności jest podstawą do ustalenia kryterium dla oceny ryzyka. Kontekst wraz z dokonaną klasyfikacją zasobów informacyjnych stanowią punkt wyjściowy do identyfikacji ryzyk oraz wynikających z nich zagrożeń.
Kolejnym elementem jest analiza zidentyfikowanych ryzyk, w której oceniamy prawdopodobieństwo wystąpienia zagrożenia oraz skutków, jakie zagrożenia może wywołać. Zidentyfikowane i ocenione ryzyka o określonym stopniu istotności zostają zarejestrowane i udokumentowane na kartach oceny ryzyka i podlegają bieżącej ocenie i monitorowaniu. Na karcie ryzyka dokumentuje się również sposoby postępowania z ryzykiem, zadania mające na celu obniżenie ryzyka, kroki jaki należy podjąć w przypadku, gdy ryzyko się zmaterializuje. Przyjmuje się, że ponowna ocena zidentyfikowanego ryzyka nie może być rzadsza niż raz na miesięcy.

4. OPIS METODY ANALIZY RYZYKA

4.1 KONTEKST DZIAŁALNOŚCI URZĘDU

Działalność Urzędu Miejskiego w Sokółce wiąże się ze spełnianiem oczekiwań wielu stron. Strony te i ich oczekiwania stanowią kontekst działalności urzędu, a oczekiwania względem przepływu i bezpieczeństwa informacji są kryteriami ryzyka, które powinno podlegać bieżącej analizie i ocenie.
Elementy stanowiące zewnętrzny i wewnętrzny kontekst organizacyjny zostały zidentyfikowane i opisane poniżej.

4.1.1 Kontekst zewnętrzny

LP/KZ	Opis	Wpływ urzędu na aspekt	Cele/ wymagania/oczekiwania względem UM w Sokółce
01	Mieszkańcy gminy Sokółka	Nie	Oczekiwanie sprawnego działania urzędu, racjonalne kosztowo realizowanie zadań administracji publicznej
02	Starostwo Powiatowe	Nie	Sprawna realizacja zadań powierzonych urzędowi
03	Urząd Marszałkowski i Urząd Wojewódzki	Nie	Sprawna realizacja zdań administracyjnych, w tym zleconych, podejmowanie działań w ramach ustalonego prawa, stanowienie racjonalnego prawa lokalnego

04	Instytucje publiczne regulujące pracę administracji (Krajowe Biuro Wyborcze, GUS, inni)	Nie	Realizacja zadań powierzonych urzędowi
05	Jednostki organizacyjne gminy (szkoły, przedszkola, OSiR, OPS, SOK, spółki gminne, ZGKiM)	Tak	Utrzymanie wsparcia dla własnych jednostek organizacyjnych, w tym zakresie dostarczania usług elektronicznych (sprawna komunikacja z urzędem)
06	Organizacje pozarządowe na terenie gminy (kluby sportowe, organizacje pożytku publicznego)	Częściowy	Wsparcie dla działalności klubów, patronat nad wydarzeniami

4.1.2 Kontekst wewnętrzny

LP/KZ	Opis	Wpływ urzędu na aspekt	Cele/ wymagania/oczekiwania względem UM w Sokółce
01	Rada Miejska w Sokółce	Częściowy	Realizacja zadań urzędu wynikający ze statutu oraz uchwał rady, nadzorowanie pracy Burmistrza oraz podległych mu jednostek organizacyjnych
02	Burmistrz i kadra kierownicza Urzędu Miejskiego w Sokółce	Tak	Bezpieczeństwo zasobów informatycznych, dostęp do bieżącej informacji zarządczej, unikanie i zapobieganie incydentom związanych z utratą bądź zniszczeniem danych
03	Pracownicy Urzędu Miejskiego w Sokółce	Tak	Bezpieczeństwo pracy użytkowników, dostępność środków wymiany informacji, uzyskanie informacji na poziomie umożliwiającym sprawne realizowanie powierzonych zadań
04	Systemy wsparcia informacji	Tak	Systemy wymiany informacji działają w oparciu o sprawną infrastrukturę sieciowo – serwerową. Wymagają utrzymania jej na poziomie pozwalającym na sprawne przekazywanie danych między aplikacjami i bazami danych a terminalami
05	Infrastruktura informatyczna (sieci, węzły komunikacyjne, serwery)	Tak	Infrastruktura informatyczna pozwala na sprawne przekazywanie danych między aplikacjami, bazami danych a użytkownikami
06	Obsługa informatyczna	Tak	Urząd ma zatrudnionego informatyka

4.2 INWENTARYZACJA AKTYWÓW INFORAMTYCZNYCH

Klasyfikacji zasobów informatycznych dokonuje się oddzielnie dla każdej jednostki organizacyjnej urzędu. Zidentyfikowane zasoby opisuje się w „Karcie klasyfikacji zasobów i aktywów informacyjnych". W klasyfikacji należy uwzględnić kto jest właścicielem danego zasobu informatycznego oraz jakie wymagania bezpieczeństwa zidentyfikowano dotychczas w celu jego zabezpieczenia.

Zidentyfikowane zasoby informacyjne poddaje się analizie pod względem ich istotności w organizacji. Określenie ich wartości dla działalności organizacji następuje poprzez przydzielenie im odpowiednich ocen w obszarze poufności (P), dostępności (D) i integralności (I). Kryteria opisano w puntach 4.2.1, 4.2.2, 4.2.3. W celu uporządkowania klasyfikacji, zasoby, które mają podobną wartość oraz podobne wymogi bezpieczeństwa można łączyć w grupy.

4.2.1 Poziom poufności

1	Informacje ogólnodostępne
2	Informacje chronione przede wszystkim ustawą o ochronie danych osobowych (z wyjątkiem art. 27 ustawy), informacje które przetwarzane są w wielu instytucjach (np. firmy telekomunikacyjne, dostawców mediów), również chronione informacje wewnętrzne
3	Informacje chronione przede wszystkim artykułem 27 ustawy o ochronie danych osobowych (tzw. wrażliwe), również informacje objęte tajemnicą, wynikającą z innych aktów prawnych (np. ordynacji podatkowej, tajemnicy bankowej, itp.). Informacje, których ujawnienie może wiązać się z sankcjami karnymi lub odszkodowawczymi oraz mogą zagrażać istnieniu firmy

4.2.2 Poziom dostępności

1	Informacje, które są konieczne do realizacji zadania, a przerwa w dostępie do nich może być dłuższa niż 5-7 dni roboczych
2	Informacje, które są konieczne do realizacji zadania, a przerwa w dostępie do nich może być dłuższa niż 3-5 dni roboczych
3	Informacje, które muszą być dostępne w sposób nieprzerwalny, brak dostępu może w skrajnych przypadkach skutkować sankcjami karnymi lub odszkodowawczymi

4.2.3 Poziom integralności

1	Naruszenie integralności informacji jest łatwe do wykrycia i naprawienia, skutki wywołane nieprawidłową informacją są łatwe do przewidzenia i naprawienia
2	Naruszenie integralności informacji jest możliwe do wykrycia i naprawienia, skutki wywołane wadliwą informacją są możliwe do skorygowania, wymaga to jednak pewnego wkładu pracy i/lub wiąże się z poniesieniem niewielkich nakładów finansowych
3	Naruszenie integralności informacji jest trudne lub wręcz niemożliwe do naprawienia, skutki wywołane wadliwą informacją wiążą się z poważnymi sankcjami (np. odszkodowawczymi lub karnymi), usunięcie lub skorygowanie skutków wiąże się z ponoszeniem znaczących nakładów finansowych

4.3 POZIOM OCHRONY INFORMACJI

Poziom ochrony jest określany na podstawie poziomu poufności, dostępności i integralności aktywu lub grupy aktywów informacyjnych. Poziom ochrony wynika z najwyżej przyznanej oceny atrybutów bezpieczeństwa dla grupy informacji (poufności, dostępności, integralności). Przyjęta skala obejmuje I, II, III poziom ochrony.

4.4 IDENTFIKACJA ZAGROŻEŃ

Dla każdego kontekstu/ grupy aktywów informacyjnych określa się podatności i zagrożenia z nich wynikające. W analizie bierzemy pod uwagę trzy grupy zagrożeń dla zasobów informacyjnych jednostki, które rozważamy w kontekście określenia ryzyka związanego z przetwarzaniem informacji.

Zagrożenia dla poufności informacji

- Poufność, właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom

Zagrożenie dla integralności informacji (nienaruszalność)

- Integralność danych, właściwość polegająca na tym, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany
- Integralność systemu, właściwość polegającą na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej

Zagrożenie dla dostępności informacji

- Dostępność, właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany (upoważniony) podmiot

4.5 ANALIZA ODDZIAŁYWANIA ZAGROŻEŃ NA BEZPIECZEŃSTWO ZASOBÓW

Badana grupa informacji/ aktywów informacyjnych analizowana jest pod kątem wpływu typowych podatności i wynikających z nich zagrożeń. Każde zagrożenie analizowane jest na okoliczność utraty poufności, integralności i dostępności opisywanej grupy informacji.

Każde zagrożenie oceniane jest w skali pięciostopniowej (od bardzo małego do bardzo dużego), według kryteriów uwzględniających wartość skutku i jego następstwa (oddziaływanie). Kryteria oceny znajdują się w „tabeli oceny oddziaływania". Oddziaływanie ryzyka oceniamy uwzględniając funkcjonujące zabezpieczenia.

TABELA OCENY ODDZIAŁYWANIA

Stopień	Skutki finansowe	Odpowiedzialność za zaistnienie incydentu	Ochrona zdrowia i bezpieczeństwo osób	Reputacja
Bardzo wysoki	od 250.000zł.	Złamanie przepisów prawa- odpowiedzialność karna, ograniczenie lub pozbawienie wolności	Utrata życia	Doniesienia medialne w całym kraju
Wysoki	od 100.000zł. do 250.000zł.	Złamanie przepisów prawa – odpowiedzialność służbowa lub finansowa	Poważne obrażenia	Pewne informacje w mediach ogólnokrajowych
Średni	od 10. 000zł. do 100. 000zł.	Złamanie przepisów prawa – odpowiedzialność służbowa	Pewne obrażenia	Pewne informacje w mediach lokalnych lub regionalnych
Niski	od 1000zł. do 10. 000zł.	Naruszenie przepisów prawa – brak odpowiedzialności	Niewielkie obrażenia	Ograniczone informacje w mediach lokalnych lub regionalnych
Bardzo niski	od 100zł. do 1000zł.	Nie ma naruszenia przepisów prawa	Niewielkie obrażenia	Ubogie informacje w mediach lokalnych lub regionalnych

4.6 ANALIZA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻEŃ

Każde z ocenianych zagrożeń dla grup informacji/aktywów jest oceniane pod kątem prawdopodobieństwa wystąpienia. Skala oceny jest pięciostopniowa (od bardzo małego do bardzo dużego). Kryteria oceny znajdują się w „tabeli oceny prawdopodobieństwa". Prawdopodobieństwo wystąpienia ryzyka oceniamy uwzględniając funkcjonujące zabezpieczenia.

TABELA OCENY PRAWDOPODOBEŃSTWA

Prawdopodobieństwo wystąpienia	Opis
Bardzo wysokie	Wydarzenie wysoce prawdopodobne, którego można się spodziewać raz w miesiącu lub częściej
Wysokie	Wydarzenie, którego zaistnienie jest dość prawdopodobne i można się go spodziewać kilka razy w roku
Średnie	Wydarzenie, którego zaistnienie jest względnie prawdopodobne, być może raz w roku
Niskie	Zdarzenie, którego zaistnienie jest mało prawdopodobne, być może raz na 3 lata
Bardzo niskie	Zdarzenie, którego zaistnienie jest wysoce nieprawdopodobne lub prawdopodobne teoretycznie

4.7 WAGA RYZYKA

Waga ryzyka określana jest w skali pięciostopniowej (od bardzo małego lub bardzo dużego). Wagę ryzyka ustala się na podstawie macierzy ryzyka, w której przyporządkowuje się ocenę prawdopodobieństwa do wpływu, jakie potencjalnie niesie ze sobą ryzyko.

TABELA MACIERZY RYZYKA

Wpływ	Bardzo wysoki	3	3	4	4	5
	Wysoki	2	3	3	4	4
	Średni	2	2	3	3	4
	Niski	1	2	2	3	3
	Bardzo niski	1	1	2	2	3
		Bardzo niskie	Niskie	Średnie	Wysokie	Bardzo wysokie
		Prawdopodobieństwo				

4.8 KRYTERIA AKCEPTACJI RYZYKA

Otrzymany wynik w skali od 1 do 5 przekłada się na ocenę wagi ryzyka. Ogólne zasady postępowania ze zidentyfikowanym ryzykiem opisane są w „tabeli ogólnych zasad wyznaczania ryzyka"

TEBELA OGÓLNYCH ZASAD WYZNACZANIA DOPUSZCZALNOŚCI RYZYKA

Waga ryzyka wg macierzy	Oszacowanie ryzyka	Dopuszczalność ryzyka	Niezbędne działania
5	Bardzo duże	Niedopuszczalne	Ryzyko krytyczne, działania mające na celu zmniejszenia ryzyka do poziomu dopuszczalnego należy podjąć natychmiast
4	Duże		Ryzyko wysokie, działania mające na celu zmniejszenie ryzyka do poziomu dopuszczalnego należy podjąć niezwłocznie. Jeżeli ryzyko występuje w związku z podjęciem nowego zadania, nie wolno go rozpocząć do momentu obniżenia poziomu ryzyka
3	Średnie	Dopuszczane	Zaleca się zaplanowanie i podjęcie działań, których celem jest zmniejszenie ryzyka
2	Małe		Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostaje najwyżej na tym samym poziomie
1	Bardzo niskie		Nie jest konieczne prowadzenie żadnych działań

4.9 KARTA ANALIZY RYZYKA BEZPIECZEŃSTWA INFORMACJI

Karta analizy ryzyka dokumentuje ryzyko wystąpienia zdarzenia negatywnie oddziałowującego na osiągnięte cele i zadania wynikające z kontekstu działalności urzędu w powiązaniu z grupami informacji opisanymi w klasyfikacji informacji. Dla każdego kontekstu/ grupy informacji sporządzamy osobną kartę. W karcie zapisujemy informacje dotyczące zasobu, jego podatności, istniejące zabezpieczenia

(techniczne, organizacyjne), wynikające z analizy ryzka zidentyfikowane zagrożenia, które realnie mogą mieć wpływ na działanie Urzędu.

4.10 REJESTR RYZYK BEZPIECZEŃSTWA INFORMACJI

Rejestr ma na celu ewidencjonowanie kart analizy ryzyka i ryzyk niedopuszczalnych oraz statusu działań mających na celu ograniczenie niedopuszczalnego ryzyka

4.11 LISTA KONTROLNA RYZYK

Lista kontrolna ryzyk jest narzędziem wspomagającym proces identyfikacji i dokumentowania procesu analizy ryzyka. Korzystanie z listy jest dobrowolne.

5. RAPORT Z ANALIZY RYZYKA

Raport z analizy ryzyka dokumentowany jest na karcie „Karta Ryzyka". W celu ułatwienia monitorowania zidentyfikowanych ryzyk, ryzyka na poziomie „średnie", „duże" i „bardzo duże" odnotowuje się w rejestrze ryzyk.

6. PLAN POSTĘPOWANIA Z RYZYKIEM

Zaplanowane działania postępowania z ryzkiem nazywają się „Planem postępowania z ryzykiem" i zapisane są w „Karcie bezpieczeństwa informacji". Dla wszystkich zasobów/działań, których poziom ryzyka będzie wyższy niż dopuszczalny, konieczne będzie wdrożenie środków ograniczających ryzyko lub zastosowanie jednej z następujących strategii postępowania:

- wdrożenie dodatkowych zabezpieczeń
- świadome zaakceptowanie przez kierownictwo ryzyka na poziomie przekraczającym próg akceptowalności,
- przeniesienie ryzyka na inny podmiot (np. ubezpieczenia)
- uniknięcie ryzyka (np. zaprzestanie użytkowania zasobu)

BURMISTRZ

Ewa Kulikowska