Warszawa, dnia 4 marca 2014 r.

Poz. 2

ZARZĄDZENIE Nr 25
MINISTRA ADMINISTRACJI I CYFRYZACJI

z dnia 31 grudnia 2013 r.

w sprawie wprowadzenia Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji

Na podstawie art. 69 ust. 1 pkt 3 w związku z art. 68 ust. 2 pkt 7 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2013 r. poz. 885 i 938) zarządza się, co następuje:

§ 1. Wprowadza się Politykę zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji stanowiącą załącznik do zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

- wz. *Stanisław HUSKOWSKI*

MINISTER ADMINISTRACJI I CYFRYZACJI

Załącznik do zarządzenia Nr 25
Ministra Administracji i Cyfryzacji
z dnia 31 grudnia 2014 r.

Polityka Zarządzania Ryzykiem
w Ministerstwie Administracji i Cyfryzacji

Rozdział 1
Postanowienia ogólne

§ 1.

1. Polityka zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji, zwana dalej „Polityką”, określa podejście do zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji, zwanym dalej „Ministerstwem”.
2. Ilekroć w Polityce jest mowa o:
   1) Planie działalności Ministra Administracji i Cyfryzacji – należy przez to rozumieć Plan działalności, o którym mowa w rozporządzeniu Ministra Finansów z dnia 29 września 2010 r. w sprawie planu działalności i sprawozdania z jego wykonania (Dz. U. Nr 187, poz. 1254) sporządzony przez Ministra Administracji i Cyfryzacji;
   2) Ministrze – należy przez to rozumieć Ministra Administracji i Cyfryzacji;
   3) Kierownictwie Ministerstwa – należy przez to rozumieć Ministra, Sekretarza Stanu, Podsekretarzy Stanu oraz Dyrektora Generalnego Ministerstwa;
   4) kierownikach komórek organizacyjnych – należy przez to rozumieć osoby kierujące pracą komórek organizacyjnych;
   5) zarządzaniu ryzykiem – należy przez to rozumieć działania podejmowane zarówno przez Kierownictwo Ministerstwa, kierowników komórek organizacyjnych, jak i pracowników, które poprzez identyfikację i analizę ryzyka oraz określenie adekwatnych reakcji na ryzyko zwiększają prawdopodobieństwo osiągnięcia celów i realizacji zadań, a także podejmowanie działań zaradczych oraz monitorowanie i przegląd ryzyk;
   6) ryzyku – należy przez to rozumieć prawdopodobieństwo wystąpienia zdarzenia, które będzie miało negatywny wpływ na realizację zadań i osiągnięcie celów;
   7) analizie ryzyka – należy przez to rozumieć systematyczne identyfikowanie czynników ryzyka i jego szacowanie;
   8) ryzyku kluczowym – należy przez to rozumieć ryzyko, które może spowodować niezrealizowanie celów strategicznych Ministerstwa, określonych w Planie działalności Ministra Administracji i Cyfryzacji lub zagrozić ich realizacji;
   9) czynniku ryzyka – należy przez to rozumieć zdarzenie, działanie, zaniechanie, które może spowodować wystąpienie ryzyka;
   10) szacowaniu ryzyka – należy przez to rozumieć proces zmierzający do wyznaczenia istotności ryzyka;
   11) istotności ryzyka – należy przez to rozumieć ocenę ryzyka określaną jako iloczyn prawdopodobieństwa wystąpienia danego ryzyka i jego wpływu na działalność Ministerstwa;
   12) akceptowalnym ryzyku – należy przez to rozumieć ryzyko, które jest możliwe do zaakceptowania i nie wymaga podejmowania działań zaradczych;
   13) mapie ryzyk – należy przez to rozumieć wykaz ryzyk, uszeregowanych według stopnia istotności, których poziom przekracza poziom akceptowalny, przy uwzględnieniu priorytetów nadanych przez Ministra;

14) właścicielu ryzyka – należy przez to rozumieć osobę odpowiedzialną za zarządzanie danym ryzykiem;
15) kontroli zarządczej – należy przez to rozumieć ogół działań podejmowanych dla zapewnienia realizacji zadań i osiągnięcia celów, w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

§ 2.

1. Celem wprowadzenia Polityki jest:
   1) zwiększenie prawdopodobieństwa osiągnięcia celów i realizacji zadań poprzez: ograniczenie potencjalnych, negatywnych skutków zdarzeń do akceptowalnego poziomu, usprawnienie procesu planowania oraz zapewnienie Kierownictwu Ministerstwa informacji o zagrożeniach realizacji zadań i osiągnięcia celów, w tym w szczególności określonych w ramach Planu działalności Ministra Administracji i Cyfryzacji;
   2) usystematyzowanie i ujednolicenie podejścia Ministerstwa do zarządzania ryzykiem;
   3) uświadomienie wpływu ryzyk towarzyszących działalności Ministerstwa na realizację zadań i osiągnięcie jego celów.
2. Polityka określa:
   1) obszar i zasady zarządzania ryzykiem;
   2) uczestników biorących udział w zarządzaniu ryzykiem powodujących zwiększenie prawdopodobieństwa osiągnięcia celów Ministerstwa;
   3) etapy zarządzania ryzykiem;
   4) ogólne zasady monitorowania i dokonywania przeglądu ryzyk oraz informowania o nich.

§ 3.

1. Polityka obejmuje członków Kierownictwa Ministerstwa i ma zastosowanie do wszystkich komórek organizacyjnych Ministerstwa oraz wszystkich pracowników zatrudnionych w Ministerstwie.

Rozdział 2
Obszar i zasady

§ 4.

1. Polityka została zdefiniowana dla następujących poziomów:
   1) strategicznego (cele ogólne);
   2) operacyjnego (cele szczegółowe).
2. Zarządzanie ryzykiem w Ministerstwie odbywa się poprzez:
   1) strategiczne zarządzanie ryzykiem oparte na rocznej identyfikacji i analizie ryzyka;
   2) operacyjne/cykliczne zarządzanie ryzykiem polegające na ciągłej identyfikacji, ocenie ryzyka i podejmowaniu działań zaradczych na bieżąco – jako element zachodzących zmian i potrzeb.
3. Zarządzanie ryzykiem realizowane jest we wszystkich obszarach działania Ministerstwa i w zakresie wszystkich komórek organizacyjnych Ministerstwa, czyli w zakresie departamentu, biura, wydziału, zespołu, stanowiska.

4. Zarządzanie ryzykiem jest wykonywane w zakresie realizacji zadań i osiągania określonych celów, wydajnego, ekonomicznego i efektywnego wykorzystania posiadanych zasobów.
5. W procesie zarządzania ryzykiem poszczególne komórki organizacyjne Ministerstwa ustalają cele szczegółowe, które są przyporządkowane corocznie do właściwych celów ogólnych, co pozwala na identyfikację ich wzajemnych powiązań.
6. Cały proces zarządzania ryzykiem jest udokumentowany zgodnie z zasadami określonymi poniżej.

Rozdział 3
Zadania i odpowiedzialność

§ 5.

1. W Ministerstwie funkcjonuje Koordynator ds. zarządzania ryzykiem, zwany dalej „Koordynatorem”.
2. Koordynator:
   1) organizuje wdrażanie zarządzania ryzykiem w Ministerstwie;
   2) współpracuje z kierownikami komórek organizacyjnych, Sekretarzem, Podsekretarzami Stanu i Dyrektorem Generalnym Ministerstwa oraz pracownikami w zakresie identyfikacji i analizy ryzyka;
   3) sporządza pisma, raporty, informacje w zakresie ryzyka dla Ministra;
   4) przygotowuje zbiorcze informacje o zaistniałych w Ministerstwie ryzykach według stopnia ich istotności jak również informacje o powziętych działaniach zaradczych;
   5) dokonuje corocznego przeglądu Polityki i uaktualnia dokumenty związane z Polityką.

§ 6.

1. Na poziomie strategicznym za realizację Polityki odpowiada Minister, poprzez:
   1) kształtowanie i wdrażanie polityki zarządzania ryzykiem oraz nadzór nad nią;
   2) identyfikowanie czynników ryzyka i ocenę ryzyka na poziomie strategicznym;
   3) zdefiniowanie obszarów działania;
   4) określenie akceptowalnego poziomu ryzyka;
   5) monitorowanie ryzyka (skuteczność zastosowania mechanizmów kontrolnych);
   6) wyznaczenie właścicieli ryzyka, w fazie strategicznego zarządzania ryzykiem;
2. W proces identyfikacji i oceny ryzyka na poziomie strategicznym włączeni są Sekretarz i Podsekretarze Stanu oraz Dyrektor Generalny Ministerstwa.
3. Minister może przypisać odpowiedzialność za zarządzanie kluczowym ryzykiem związanym z głównym celem Ministerstwa – właściwemu merytorycznie Sekretarzowi, Podsekretarzowi Stanu lub Dyrektorowi Generalnemu Ministerstwa.
4. W przypadku ryzyka dotyczącego obszaru realizowanego przez więcej niż jedną komórkę organizacyjną Ministerstwa, właścicielem ryzyka jest członek Kierownictwa Ministerstwa, dla którego ryzyko jest najbardziej istotne.
5. Właściciel ryzyka jest uprawniony do powołania zespołu do spraw szacowania ryzyka lub do przygotowania planów postępowania z ryzykiem. O powołaniu zespołu właściciel ryzyka każdorazowo zawiadamia Koordynatora.

§ 7.

1. Na poziomie operacyjnym za zarządzanie ryzykiem odpowiadają kierownicy komórek organizacyjnych poprzez:
   1) identyfikację i udokumentowanie czynników ryzyka, które są istotne dla osiągnięcia celów operacyjnych, w odniesieniu do zidentyfikowanych obszarów działania;
   2) ocenę istotności ryzyka w odniesieniu do realizowanych zadań, z uwzględnieniem prawdopodobieństwa oraz potencjalnych skutków ryzyka wywołanych tymi czynnikami (zagrożeniami);
   3) prowadzenie działań związanych z postępowaniem z ryzykiem;
   4) monitorowanie ryzyka w zakresie swojego obszaru działania, w tym funkcjonowania mechanizmów kontrolnych pod kątem ich adekwatności i skuteczności, a także wszelkich odstępstw od istniejących procedur;
   5) prowadzenie rejestru odstępstw od obowiązujących zasad i procedur, zgodnie z załącznikiem nr 1 do Polityki, oraz ich analizę;
   6) przedstawianie Koordynatorowi informacji o działaniach związanych z zarządzaniem ryzykiem;
   7) ponowne przeprowadzenie szacowania ryzyka lub czynności związanych z postępowaniem z ryzykiem, w przypadku kiedy Minister uzna to za konieczne.

Rozdział 4

Etapy

§ 8.

1. Identyfikacja czynników ryzyka odbywa się z wykorzystaniem arkusza stanowiącego załącznik nr 2 do Polityki w odniesieniu do zdefiniowanych na poziomie strategicznym obszarów działania.
2. Wykaz obszarów stanowi załącznik nr 3 do Polityki.
3. Identyfikacja czynników ryzyka odbywa się na szczeblu każdej komórki organizacyjnej Ministerstwa w odniesieniu do celów Ministerstwa z uwzględnieniem mierników ich realizacji.
4. Zidentyfikowane ryzyko należy opisać i przyporządkować do określonej poniżej kategorii ryzyka:
   1) zarządzanie;
   2) finanse;
   3) bezpieczeństwo;
   4) czynniki zewnętrzne;
   5) przepisy i procedury;
   6) działalność operacyjna.
5. W procesie identyfikacji czynników ryzyka, należy wziąć w szczególności pod uwagę ryzyka związane m.in. ze zmianami zachodzącymi w Ministerstwie lub jego otoczeniu, z systemami informatycznymi, ryzyka o charakterze finansowym, jak również zagrażające wizerunkowi Ministerstwa jako urzędu administracji publicznej sprawnego i przyjaznego obywatelom, związane z członkostwem Polski w Unii Europejskiej oraz ryzyko korupcji.
6. Pracownicy Ministerstwa mają obowiązek zgłaszać za pośrednictwem elektronicznego systemu obiegu dokumentów swoim przełożonym wszelkie odstępstwa od przyjętych w Ministerstwie zasad i procedur, zgodnie z załącznikiem nr 1 do Polityki.

§ 9.

1. Po określeniu celów, obszarów działania, zadań, kategorii ryzyka i zidentyfikowaniu do nich czynników ryzyka, zidentyfikowane ryzyko podlega analizie mającej na celu oszacowanie wpływu, tj. prawdopodobieństwa wystąpienia ryzyka, a także skutku wystąpienia danego zdarzenia. Umożliwia to określenie istotności (znaczenia) każdego ryzyka.
2. Dokonując szacowania ryzyka należy wziąć pod uwagę uwarunkowania mające wpływ na prawdopodobieństwo i skutek wystąpienia zdarzenia, zgodnie z załącznikiem nr 4 do Polityki.
3. Przy ocenie prawdopodobieństwa wystąpienia zdarzenia należy wziąć pod uwagę istniejące mechanizmy kontrolne, ich skuteczność i poziom wdrożenia.
4. Do szacowania prawdopodobieństwa stosuje się metodę punktową, zgodnie z poniższą skalą:

Prawdopodobieństwo wystąpienia zagrożenia		
Ocena	**Punkty**	**Opis**
Rzadkie	1	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz lub nie zdarzy się w ciągu roku.
Mało prawdopodobne	2	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się dwa lub trzy razy w ciągu roku.
Możliwe	3	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się kilkakrotnie w ciągu roku.
Prawdopodobne	4	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się więcej niż kilkakrotnie w ciągu roku.
Prawie pewne	5	Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku.

5. Przy ocenie skutków należy wziąć pod uwagę zarówno skutki finansowe, jak i pozafinansowe, tj. utrata reputacji, konsekwencje prawne, utrata szansy, opóźnienia, obniżenie jakości pracy.
6. Do szacowania skutku stosuje się metodę punktową, zgodnie z poniższą skalą:

Skutek związany z danym zagrożeniem		
Ocena	**Punkty**	**Opis**
Nieznaczny	1	Zdarzenie objęte ryzykiem powoduje nieznaczne zakłócenie lub opóźnienie w wykonywaniu zadań, nie wpływa na wizerunek jednostki. Skutki zdarzenia można łatwo usunąć.
Mały	2	Zdarzenie objęte ryzykiem powoduje małe zakłócenie lub opóźnienie w wykonywaniu zadań, częściowo wpływa na wizerunek jednostki. Skutki zdarzenia można usunąć.
Średni	3	Zdarzenie objęte ryzykiem powoduje średnią stratę posiadanych zasobów, małą stratę finansową, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, wizerunek jednostki.

		Z wystąpieniem zdarzenia może się wiązać trudny proces przywracania stanu poprzedniego.
Duży	4	Zdarzenie objęte ryzykiem powoduje poważną stratę posiadanych zasobów, średnia stratę finansową, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, wizerunek jednostki. Z wystąpieniem zdarzenia wiąże się trudny proces przywracania stanu poprzedniego.
Krytyczny	5	Zdarzenie objęte ryzykiem powoduje uszczerbek mający krytyczny lub bardzo duży wpływ na realizację kluczowych zadań lub osiąganie założonych celów, poważny uszczerbek w zakresie jakości wykonywanych zadań, poważną stratę finansową albo niekorzystny wpływ na wizerunek jednostki. Z wystąpieniem zdarzenia wiąże się długotrwały i trudny proces przywracania stanu poprzedniego.

7. Istotność ryzyka określa się zgodnie z poniższą skalą punktową:

Istotność ryzyka	
Ocena	**Punktacja**
Niska	1 – 5
Średnia	6 – 10
Wysoka	12 – 16
Bardzo wysoka	20 – 25

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Graficzne przedstawienie analizy ryzyka

8. Ryzyko niskie jest ryzykiem akceptowalnym.
9. Uzyskane wyniki podlegają dalszej analizie pod kątem możliwości ograniczenia ryzyka.
10. Dokument, o którym mowa w § 8 ust. 1, wypełniany jest na poziomie operacyjnym i podlega akceptacji kierowników komórek organizacyjnych.
11. Dokument przekazywany jest do Koordynatora za pośrednictwem elektronicznego systemu obiegu dokumentów nie później niż do dnia 31 grudnia.
12. Koordynator opracowuje zestawienia zbiorcze z komórek organizacyjnych zgodnie z właściwością wynikającą z podległości, które następnie przekazuje w terminie do dnia 15 stycznia właściwym członkom Kierownictwa Ministerstwa.

§ 10.

1. Członkowie Kierownictwa Ministerstwa dokonują analizy ryzyka na szczeblu strategicznym w terminie 14 dni od dnia otrzymania zestawienia zbiorczego, o którym mowa w § 9 ust. 12, według zasad określonych w § 9.
2. Członkowie Kierownictwa Ministerstwa mogą identyfikować dodatkowe czynniki ryzyka nieuwzględnione w procesie identyfikacji na poziomie operacyjnym.
3. Dokumentowanie procesu, o którym mowa w ust. 1, odbywa się zgodnie z załącznikiem nr 2 do Polityki.
4. Po sporządzeniu analizy ryzyka na szczeblu strategicznym, członkowie Kierownictwa Ministerstwa przekazują dokumenty do Koordynatora.

§ 11.

1. Po udokumentowaniu procesu identyfikacji i analizy ryzyka na poziomie operacyjnym oraz przez członków Kierownictwa Ministerstwa na poziomie strategicznym, Koordynator opracowuje zestawienie zbiorcze ujednolicając i kumulując powtarzające się czynniki ryzyka.
2. Zestawienie, o którym mowa w ust. 1, Koordynator przekazuje Ministrowi w terminie określonym w § 14 ust. 1.
3. Minister nadaje priorytet poszczególnym czynnikom ryzyka.
4. Przyjęto czterostopniową skalę priorytetu: bardzo wysoki, wysoki, średni, niski, przypisując każdemu odpowiednio wagę: 4, 3, 2, 1.
5. Wyniki analizy ryzyka uwzględniają priorytety Ministra.
6. Minister, stosownie do potrzeb, przedstawia na posiedzeniu Kierownictwa Ministerstwa informacje o ryzykach, które mogą zagrozić realizacji głównych celów Ministerstwa oraz o podjętych i przewidywalnych działaniach zaradczych związanych z tymi ryzykami.
7. W razie konieczności Minister wyznacza właścicieli ryzyka.

Rozdział 5
Interpretacja wyników i zarządzanie

§ 12.

1. W Ministerstwie zdefiniowano cztery poziomy ryzyka: niskie, średnie, wysokie, bardzo wysokie:
   1) ryzyko niskie zawiera się w przedziale do 25% maksymalnego możliwego poziomu ryzyka,
   2) ryzyko średnie zawiera się w przedziale od 26%-50% maksymalnego możliwego poziomu ryzyka,
   3) ryzyko wysokie zawiera się w przedziale od 51%-75% maksymalnego możliwego poziomu ryzyka,
   4) ryzyko bardzo wysokie zawiera się w przedziale od 76%-100% maksymalnego możliwego poziomu ryzyka.

2. Uzyskane w procesie analizy ryzyka końcowe wyniki wskazują na poziom ryzyka wywołanego określonym czynnikiem ryzyka.
3. Kierując się danymi zawartymi w arkuszach identyfikacji Koordynator przygotowuje mapę ryzyka.
4. Koordynator rozsyła mapę ryzyka członkom Kierownictwa Ministerstwa i kierownikom komórek organizacyjnych.

§ 13.

1. Ryzyko jest akceptowalne wtedy, gdy wartość jest nie większa niż 25% maksymalnego poziomu ryzyka.
2. Przyjęto następujące podstawowe zasady akceptowalności ryzyka:
   1) ryzyko niskie – ryzyko akceptowalne, które należy monitorować i w miarę potrzeb sprawdzać, czy jest ono prawidłowo kontrolowane;
   2) ryzyko średnie – może wywierać poważny wpływ na działalność Ministerstwa, należy monitorować i rozważyć potrzebę działań zaradczych i wprowadzenie dodatkowych mechanizmów kontroli mając na uwadze koszty wprowadzenia kontroli, można tolerować średni poziom, gdy koszty zapobiegania ryzyka są zbyt wysokie, ale należy na bieżąco sprawdzać poziom ryzyka. Za monitoring ryzyka i ewentualne zaprojektowanie mechanizmów kontrolnych odpowiedzialny jest właściciel ryzyka;
   3) ryzyko wysokie – może potencjalnie wpłynąć na działalność Ministerstwa, wymaga wprowadzenia przez kierownictwo operacyjne działań zaradczych i uzupełnienia wewnętrznych mechanizmów kontrolnych, które ograniczą prawdopodobieństwo wystąpienia ryzyka. Decyzję o tolerowaniu (akceptacji) ryzyka może podjąć tylko Minister;
   4) ryzyko bardzo wysokie – stanowi poważne zagrożenie dla działalności Ministerstwa lub osiągnięcia przez niego celów działania. Potrzebne jest natychmiastowe działanie, poprzez wprowadzenie silnych mechanizmów kontroli. Podlega ciągłemu monitoringowi, nie może być tolerowane. Kierownictwo operacyjne jest zobowiązane do zaprojektowania mechanizmów ograniczających poziom ryzyka bardzo wysokiego.
3. Ryzyko wysokie i bardzo wysokie stanowi ryzyko kluczowe dla działalności Ministerstwa.
4. W stosunku do każdego ryzyka przekraczającego poziom akceptowalny podejmuje się właściwe działania:
   1) zapobieganie – czyli działania polegające na zmniejszeniu poziomu ryzyka do akceptowalnego poziomu, np. poprzez wzmocnienie mechanizmów kontroli (procedury, wytyczne, zasady, nadzór, itp.) w ramach realizowanego zadania,
   2) przeniesienie ryzyka na inną instytucję, w tym ubezpieczyciela,
   3) tolerowanie ryzyka – gdy istnieją określone trudności/ograniczenia w przeciwdziałaniu ryzyku, a także koszty podjętych działań mogą przekroczyć przewidywalne korzyści,
   4) unikanie – zaprzestanie/zawieszenie działań rodzących ryzyko.
5. Przy wyznaczaniu akceptowalnego poziomu każdego ryzyka Kierownictwo Ministerstwa wyznacza stopień ryzyka, jakie gotowe jest przyjąć, z uwzględnieniem sytuacji Ministerstwa oraz wielkości kosztów ograniczenia danego ryzyka.
6. O sposobie postępowania odnośnie do każdego zidentyfikowanego ryzyka, w szczególności w zakresie podejmowanych działań, decyduje właściciel ryzyka.
7. Minister może podjąć decyzję o akceptacji ryzyka na poziomie niskim, średnim i wysokim i nie podejmowaniu działań zaradczych.
8. Kierownicy komórek organizacyjnych na bieżąco podejmują działania zaradcze dotyczące ryzyk wynikających z odstępstw od obowiązujących zasad i procedur.

Rozdział 6
Raportowanie

§ 14.

1. Koordynator przedstawia Ministrowi nie rzadziej niż raz na rok w terminie do dnia 28 lutego informację o zagrożeniach w realizowanych zadaniach obarczonych największym ryzykiem w Ministerstwie oraz o podjętych na szczeblu komórek organizacyjnych działaniach zaradczych. Wraz z wymienioną informacją, Koordynator przedstawia wstępne propozycje rekomendacji dotyczących postępowania z ryzykiem w przypadkach, gdy kompetencje do podjęcia działań w tym zakresie należą do Ministra.
2. Koordynator przekazuje na bieżąco innym właścicielom obszarów ryzyka informacje o tych ryzykach, które wykraczają poza jeden obszar funkcjonowania Ministerstwa.
3. Wyniki identyfikacji i analizy ryzyka wykorzystywane będą przez audytora wewnętrznego na etapie przygotowywania rocznego planu audytu wewnętrznego w Ministerstwie.
4. Wszyscy pracownicy mają prawo i obowiązek raportowania o negatywnych zdarzeniach kierownikom komórek organizacyjnych lub członkom Kierownictwa Ministerstwa oraz wskazanie potencjalnych źródeł zagrożeń. Na podstawie posiadanych informacji członkowie Kierownictwa Ministerstwa mają obowiązek podjąć działania w zakresie swoich uprawnień lub zaproponować Ministrowi działania zmierzające do usunięcia wskazanych problemów.

Rozdział 7
Monitorowanie ryzyka i nadzór

§ 15.

1. W Ministerstwie proces monitorowania ryzyka jest procesem ciągłym realizowanym przez Kierownictwo Ministerstwa na każdym szczeblu zarządzania, który pozwala na podejmowanie decyzji w odpowiednim czasie.
2. Kierownictwo Ministerstwa wspiera wszelkie działania pracowników przyjmujących odpowiedzialność za ryzyko.
3. Kierownicy komórek organizacyjnych prowadzą monitoring funkcjonowania mechanizmów kontrolnych pod kątem ich adekwatności, efektywności i skuteczności. W ramach monitoringu dokonywany jest przegląd aktualności ryzyk, aktualności przypisanej do ryzyk oceny, a także przegląd mechanizmów kontrolnych i ich skuteczności.
4. W przypadku wystąpienia istotnych zmian w zakresie zidentyfikowanych ryzyk lub wyników ich szacowania należy bezzwłocznie powiadomić o nich Koordynatora.
5. Za działania mające na celu sprawny monitoring na szczeblu strategicznym odpowiada Koordynator.

§ 16.

1. Niezależną ocenę zarządzania ryzykiem w Ministerstwie przeprowadza audytor wewnętrzny Ministerstwa.
2. Ocenę zarządzania ryzykiem mogą przeprowadzić również audytorzy zewnętrzni.

Rozdział 8
Aktualizacja Polityki

§ 17.

1. Polityka wraz z załącznikami podlega corocznym przeglądom, w terminie do dnia 31 maja, dokonywanym w celu ich aktualizacji.
2. Każda aktualizacja Polityki podlega akceptacji Ministra.

Załącznik nr 1

do Polityki Zarządzania Ryzykiem w MAC

Rejestr odstępstw od przyjętych zasad i procedur

Komórka organizacyjna:						
L.p.	**Rodzaj odstępstwa, naruszona zasada, procedura**	**Data ujawnienia**	**Osoba zgłaszająca naruszenie**	**Komórka w której ujawniono odstępstwo**	**Przyczyny**	**Skutki**

Załącznik nr 2

do Polityki Zarządzania Ryzykiem w MAC

…….

wypełnia

Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałania ryzykom związanym z osiągnięciem celów[1]

Określenie ryzyka dla celów/zadań ujętych w Planie działalności komórki organizacyjnej											Reakcja na ryzyko
Lp.	**cel ogólny**	**cel szczegółowy/ zadanie[2]**	**obszar działania**	**kategoria ryzyka**	**opis ryzyka**	**prawdopodobieństwo[3]**	**skutek[4]**	**istotność ryzyka[5]**	**priorytet Ministra**	**właściciel ryzyka[6]**	**przyjęta metoda przeciwdziałania ryzyku (mechanizm kontroli wewnętrznej)[7]**
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**	**11.**	**12.**
1.											
2.											
…											

…….

data sporządzenia

……

akceptował

[1]Arkusz wypełnia się na poziomie operacyjnym i strategicznym w oparciu o cele ogólne wskazane w rocznym Planie działalności Ministra Administracji i Cyfryzacji.

[2]Należy wskazać kolejno cele/zadania do osiągnięcia przez komórkę organizacyjną, przyporządkowując je odpowiednio do celów ogólnych.

[3]Prawdopodobieństwo ocenia się w skali 1 (rzadkie), 2 (mało prawdopodobne), 3 (możliwe), 4 (prawdopodobne), 5 (prawie pewne) z uwzględnieniem istniejących mechanizmów kontrolnych.

[4] Skutek ocenia się w skali 1 (nieznaczny), 2 (mały), 3 (średni), 4 (duży), 5 (krytyczny) z uwzględnieniem istniejących mechanizmów kontrolnych.

[5] Istotność ryzyka - iloczyn liczb wyrażających wartość punktową skutku i prawdopodobieństwa; przy ustalonej skali istotność będzie wahała się pomiędzy 1 (1x1) a 25 (5x5); akceptowalny jest poziom istotności 1, 2, 3, 4 i 5.

[6] Osoba odpowiedzialna za zarządzanie ryzykiem, posiadająca uprawnienia i kompetencje do podjęcia działań zaradczych w stosunku do ryzyka, którym zarządza. Na poziomie operacyjnym właścicielem ryzyka jest kierownik komórki organizacyjnej, na poziomie strategicznym właściciele ryzyka wyznacza Minister.

[7]Należy wskazać metodę przeciwdziałania ryzyku w przypadku, gdy istotność ryzyka została oceniona na poziomie wyższym niż akceptowalny (powyżej 5).

Załącznik nr 3
do Polityki Zarządzania Ryzykiem w MAC

Wykaz obszarów działania wyodrębnionych w MAC obejmuje w szczególności:

1. **Legislację.**
2. **Otoczenie prawne.**
3. **Orzecznictwo.**
4. **Zamówienia publiczne.**
5. **Budżet i finanse.**
6. **Kadry i szkolenia.**
7. **Informatykę.**
8. **Bezpieczeństwo i ochronę informacji.**
9. **Obsługę administracyjno-techniczną.**
10. **Informację i komunikację.**
11. **Realizację projektów finansowanych z Unii Europejskiej.**
12. **Przeprowadzanie konkursów i udzielanie dotacji.**

Załącznik nr 4

do Polityki Zarządzania Ryzykiem w MAC

KATEGORIE RYZYKA I LISTA CZYNNIKÓW RYZYKA

I. Czynniki wpływające na prawdopodobieństwo wystąpienia danego zagrożenia:

1. Zarządzanie i organizacja

- Czy kompetencje, zadania i odpowiedzialność pracowników są jasno i jednoznacznie określone?
- Czy zdefiniowano zadania wrażliwe?
- Czy istnieje transparentny i obiektywny system wynagradzania i motywowania pracowników?
- Czy zarobki pracowników są adekwatne do powierzonych im zadań i obowiązków?
- Czy występuje duża rotacja pracowników?
- Czy kwalifikacje pracowników i kierownictwa odpowiadają charakterowi wykonywanych obowiązków?
- Czy warunki pracy (pomieszczenia, wyposażenie) są odpowiednie do wykonywanych zadań?
- Czy organizacja przywiązuje dużą wagę do kwestii etyki i morale pracowników?
- Czy pracownicy mają możliwość podejmowania dodatkowego zatrudnienia/zajęć zarobkowych?

2. Finanse

- Jaka jest wielkość, rodzaj dokonywanych operacji?
- Czy prowadzona jest na bieżąco sprawozdawczość i czy jest analizowana pod kątem nieprawidłowości?
- Czy występują zmiany systemu księgowego?
- Czy jednoznacznie określone są pełnomocnictwa do dysponowania środkami publicznymi?
- Czy powierzono uprawnienia pracownikom w zw. z gospodarką finansową?

3. Bezpieczeństwo

- Czy budynek i poszczególne pomieszczenia są odpowiednio zabezpieczone przed dostępem osób nieupoważnionych?
- Czy dostęp osób z zewnątrz jest monitorowany i dokumentowany (księgi gości, telewizja przemysłowa)?
- Czy spotkania z osobami z zewnątrz odbywają się w otwartych i monitorowanych pomieszczeniach?
- Czy dostęp do dokumentów jest zabezpieczony i odpowiednio określane są prawa dostępu do dokumentów dla poszczególnych pracowników?
- Czy korzystanie z dokumentów jest rejestrowane/dokumentowane? Czy istnieją procedury korzystania z dokumentów niejawnych?

- Czy sieci i zasoby informatyczne są prawidłowo zabezpieczone przed nieuprawnionym dostępem (za pomocą haseł, certyfikatów)?
- Czy dostęp do sieci i zasobów informatycznych jest dokumentowany (w postaci logów)?

4. Czynniki zewnętrzne

- Czy jednostka ma kontakt z osobami z zewnątrz (w szczególności lobbystami, klientami, wnioskodawcami itp.)?
- Czy przepisy odnoszące się do działalności jednostki podlegają częstym zmianom?
- Czy jednostka jest narażona na naciski polityczne?

5. Przepisy i procedury

- Czy działalność jednostki jest opisana procedurami i czy są one przestrzegane i dokumentowane?
- Czy przepisy regulujące działalność jednostki są jasne i przejrzyste?
- Czy prowadzony jest regularnie audyt? Czy opisane są ścieżki audytu?
- Czy działalność jest udokumentowana, rejestrowana poddawana systematycznej kontroli wewnętrznej?
- Czy została opracowana procedura zarządzania zmianami?

II. Możliwe skutki wystąpienia danego zagrożenia.

- możliwość utraty reputacji/zaufania obywateli,
- skutki finansowe dla budżetu,
- skutki finansowe dla pracowników,
- zaburzenia w funkcjonowaniu jednostki – niewywiązanie lub nieprawidłowe wywiązywanie się z powierzonych zadań,
- reperkusje na arenie międzynarodowej,
- dodatkowe, nieplanowane kontrole,
- wywołanie zmian organizacyjnych,
- odpowiedzialność dyscyplinarna,
- utrata możliwości ubiegania się o środki unijne,
- konsekwencje prawne.