Załącznik Nr 18 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Procedura zarządzania ryzykiem z obszaru bezpieczeństwa informacji w Urzędzie Miasta Szczecin

§ 1. 1. Realizacja zadań nałożonych na Urząd wymaga spójnego, odpowiedzialnego i kompleksowego podejścia do zdarzeń, które występują w trakcie wykonywanych przez użytkowników zadań oraz mają wpływ na osiąganie zakładanych celów.

2. Obowiązującym standardem działania Urzędu jest określenie prawdopodobieństwa wystąpienia danego zdarzenia oraz przygotowanie się do następstwa (skutku) jego wystąpienia, nazywane procedurą zarządzania ryzykiem.

1. Procedurą zarządzania ryzykiem objęte są wszystkie działania Urzędu, wszyscy pracownicy zatrudnieni w Urzędzie realizujący wyznaczone im zadania.

§ 2. Użyte w procedurze określenia mają następujące znaczenie:

1) ryzyko - prawdopodobieństwo wystąpienia zdarzenia, które będzie miało wpływ na osiąganie założonych celów i realizację zadań nałożonych na Urząd,

2) akceptowany poziom ryzyka - ustalony w zarządzeniu poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku,

3) zarządzanie ryzykiem - podejmowanie decyzji i realizacja działań prowadzących do osiągnięcia przez Urząd akceptowanego poziomu ryzyka.

§ 3. 1. Celem zarządzania ryzykiem w Urzędzie jest:

1) usprawnienie procesu planowania,

2) zwiększenie prawdopodobieństwa osiągania założonych celów i realizacji nałożonych zadań,

3) zapewnienie odpowiednich mechanizmów kontroli zarządczej,

4) zapewnienie Prezydentowi wczesnej informacji o zagrożeniach dla realizacji wyznaczonych celów i zadań.

2. Proces zarządzania ryzykiem obejmuje następujące czynności:

1) identyfikację ryzyka,

2) ocenę zagrożeń i projektowanie czynności kontrolnych,

3) monitorowanie występowania zagrożeń (stanów niepożądanych),

4) podejmowanie decyzji i działań korygujących (lub rozwiązanie problemów).

§ 4. 1. Identyfikacja ryzyka polega na określeniu możliwych zdarzeń, które mogą (choć nie muszą) wystąpić jako przeszkody w osiąganiu celów i realizacji zadań Urzędu.

2. Podczas identyfikacji ryzyka należy przeanalizować:

1) cele i zadania realizowane przez poszczególnych pracowników,

2) realizację budżetu Urzędu,

3) zagrożenia związane z osiąganiem celów, realizowaniem zadań i budżetu Urzędu, ich przyczyny oraz skutki.

3. Przy identyfikacji ryzyka stosuje się ich kategoryzację.

2. W zakresie bezpieczeństwa procesu przetwarzania informacji ustala się następujące kategorie (obszary) ryzyka:

1) ryzyko dotyczące zasobów ludzkich,

2) ryzyko teleinformatyczne

3) ryzyko związane z bezpieczeństwem fizycznym Urzędu

4) ryzyko dotyczące ciągłości działania Urzędu

3. Identyfikację ryzyka w poszczególnych kategoriach (obszarach) przeprowadza się na podstawie:

1) posiadanego doświadczenia i prognoz na przyszłość, wykorzystując informacje wynikające z oceny zdarzeń z przeszłości oraz sporządzonych prognoz na przyszłość,

2) „burzy mózgów", opartej na uczestnictwie kierowników działów posiadających kompleksową wiedzę na temat działalności Urzędu.

3) Przeprowadzonych działań testowych (np.: testy socjotechniczne, wysyłanie fałszywych wiadomości e- mail)

§ 5. 1. Ocena ryzyka polega na określeniu wpływu i prawdopodobieństwa wystąpienia ryzyka, a następnie ustaleniu jego istotności według zasad określonych w § 5.

2. Określenie wpływu ryzyka polega na określeniu przewidywanych skutków, jakie będzie miało dla realizacji zadania, osiągania celu i realizacji budżetu Urzędu, wystąpienie zdarzenia objętego ryzykiem. Do określenia wpływu ryzyka ustala się następującą skalę ocen:

1) katastrofalny (5 pkt): ogromna strata finansowa, brak realizacji kluczowych celów, doniesienia prasowe w całym kraju,

2) poważny (4 pkt): duża strata finansowa, brak realizacji kluczowego celu, pewne informacje w mediach ogólnokrajowych,

3) średni (3 pkt): strata finansowa, zakłócenia w działalności, pewne informacje w mediach lokalnych lub regionalnych,

4) mały (2 pkt): mała strata finansowa, niewielkie zakłócenia w działalności, ograniczone informacje w mediach lokalnych lub regionalnych,

5) nieznaczny (1 pkt): niewielka strata finansowa, krótkotrwałe zakłócenia w działalności, ubogie informacje w mediach lokalnych lub regionalnych.

3. Określenie prawdopodobieństwa wystąpienia ryzyka polega na określeniu przewidywanej częstotliwości występowania zdarzenia objętego ryzykiem w trakcie roku. Do określenia prawdopodobieństwa wystąpienia ryzyka ustala się następującą skalę ocen:

Punktacja	1	2	3	4	5
Opis	Rzadkie	Mało prawdopodobne	Średnie	Prawdopodobne	Prawie pewne
Prawdopodobieństwo	0-20%	21-40%	41-60%	61-80%	81-100%

§ 6. 1. W oparciu o dokonaną ocenę wpływu i prawdopodobieństwa wystąpienia ryzyka ustalany jest poziom istotności ryzyka.

2. Ustala się następujące poziomy istotności ryzyka:

1) ryzyko nieakceptowalne – ryzyko, którego iloczyn wpływu na organizację oraz prawdopodobieństwo jego wystąpienia wynosi 15 do 25 pkt,

2) ryzyko analizowane – ryzyko, którego iloczyn wpływu na organizację oraz prawdopodobieństwo jego wystąpienia wynosi 5 do 12 pkt

3) ryzyko nieznaczne – ryzyko, którego iloczyn wpływu na organizację oraz prawdopodobieństwo jego wystąpienia wynosi 1 do 4 pkt

§ 7. 1. Ryzykiem akceptowanym jest ryzyko nieznaczne.

2. Ryzyka umiarkowane i poważne wymagają ustalenia i podjęcia działań ograniczających je do poziomu akceptowanego poprzez zmniejszenie ich wpływu lub prawdopodobieństwa wystąpienia (redukowanie ryzyku).

§ 8. 1. Metodami przeciwdziałania ryzyku są:

1) kontrolowanie ryzyka - stosowanie mechanizmów kontroli zarządczej (kontrolowanie ryzyka, plan rezerwowy),

2) unikanie ryzyka - przekazanie ryzyka podmiotowi zewnętrznemu np. w drodze ubezpieczenia.

3) redukowanie ryzyka - wdrażanie środków redukujących poziom ryzyka do akceptowalnego.

2. W celu określenia metody przeciwdziałania ryzyku należy przeanalizować:

1) przyczyny (źródła) oraz skutki ryzyka,

2) istniejące mechanizmy kontroli stosowane w celu ograniczenia lub uniknięcia ryzyka,

3) skuteczność mechanizmów kontroli (tj. określenie, w jakim zakresie mechanizmy kontroli ułatwiają lub utrudniają realizację ustalonych celów i zadań).

§ 9. 1. Identyfikacji i oceny ryzyka oraz ustalenia metody przeciwdziałania ryzyku dokonuje się raz w roku w terminie do 15 grudnia roku poprzedzającego.

2. Na podstawie dokonanej identyfikacji i oceny ryzyka oraz określenia metody przeciwdziałania ryzyku, kierownicy oraz pracownicy na samodzielnych stanowiskach pracy wypełniają „Arkusze identyfikacji, oceny oraz określenia metody redukowania ryzyk w UM Szczecin zwane dalej „arkuszami", według wzoru stanowiącego **Załącznik nr 19** do Zarządzenia.

3. Odnotowania w arkuszach wymagają wszystkie zidentyfikowane ryzyka, natomiast dla ryzyka przekraczającego akceptowany poziom ryzyka (ryzyka poważne i umiarkowane) należy podać planowane metody ograniczania go do akceptowanego poziomu.

1. Arkusze przedkładane są Dyrektorowi WInf w terminie wskazanym w ust. 1.

2. Dyrektor WInf w terminie do 15 stycznia każdego roku sporządza zbiorczy „Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku w Urzędzie Miasta Szczecin" oraz planowane metody ograniczania ryzyka poważnego i umiarkowanego do akceptowanego poziomu i przedstawia go do zatwierdzenia Prezydentowi Miasta.

§ 10. Osoby sporządzające arkusze, o których mowa w § 9 ust. 2, zapewniają stosowanie metod przeciwdziałania ryzyku ustalonych w arkuszach, a w razie zaistniałej potrzeby przygotowują projekty stosownych aktów wewnętrznych określających mechanizmy kontroli i przedstawiają je do zatwierdzenia Dyrektorowi WInf.

§ 11. 1. Zidentyfikowane ryzyko oraz ustalone metody jego ograniczania do akceptowanego poziomu są na bieżąco monitorowane przez Dyrektora WInf, ABI oraz kierowników, którzy oceniają poziom zidentyfikowanego ryzyka oraz skuteczność stosowanych metod jego ograniczania,

2. Wyniki oceny, o której mowa w ust. 1, wykorzystywane są do poprawy efektywności zarządzania ryzykiem oraz usprawnienia systemu kontroli zarządczej.