ZARZĄDZENIE NR 128/2015
BURMISTRZA MIASTA I GMINY KĄTY WROCŁAWSKIE

z dnia 14 maja 2015 r.

w sprawie ustanowienia procedury zarządzania ryzykiem w ramach Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy Kąty Wrocławskie.

Na podstawie § 20. 1. 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.2012.526 z późn. zm.) zarządzam, co następuje:

§ 1. Wprowadzam do stosowania w Urzędzie Miasta i Gminy w Kątach Wrocławskich procedurę zarządzania ryzykiem w ramach Systemu Zarządzania Bezpieczeństwem Informacji.

§ 2. Szczegółowa treść procedury zarządzania ryzykiem w ramach Systemu Zarządzania Bezpieczeństwem Informacji stanowi załącznik nr 1 do zarządzenia.

§ 3. Nadzór nad wykonaniem zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Miasta i Gminy Kąty Wrocławskie

BURMISTRZ
mgr inż. Antoni Kopeć

Antoni Kopeć

Procedura Zarządzania Ryzykiem w ramach Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy Kąty Wrocławskie

1. Procedura określa zasady i tryb zarządzania ryzykiem w ramach Systemu Zarzadzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy Kąty Wrocławskie.

2. Ilekroć w procedurze oraz innych dokumentach SZBI jest mowa o:

1) **Urzędzie** – należy przez to rozumieć Urząd Miasta i Gminy Kąty Wrocławskie,
2) **Wydziałach** - należy przez to rozumieć: wydziały, zespoły i samodzielne stanowiska pracy,
3) **Kierownikach** – należy przez to rozumieć: Zastępcę Burmistrza, Sekretarza, Skarbnika, **Kierowników wydziałów** oraz osoby zatrudnione na samodzielnych stanowiskach pracy,
4) **Akceptowanym poziomie ryzyka** - należy przez to rozumieć ustalony poziom ryzyka przy, którym nie jest wymagane podejmowanie działań przeciwdziałających ryzyku,
5) **Aktywach informacyjnych** – należy przez to rozumieć każdy nośnik i zapisaną na nim informację (dokument, dysk, urządzenie) oraz każdy inny zasób mający wpływ na zachowanie poufności, dostępności i integralności informacji i zapewniający ciągłość działania Urzędu (np. UPS),
6) **Analizie ryzyka** – należy przez to zrozumieć proces, dążący do poznania charakteru **ryzyka** oraz określenia **poziomu ryzyka** w którym poddaje się ocenie zidentyfikowane ryzyko w zakresie możliwych skutków i prawdopodobieństwa wystąpienia zdarzenia,
7) **Czynnikach ryzyka** – należy przez to zrozumieć każde zdarzenie, które będzie miało wpływ na zachowanie poufności, dostępności i integralności informacji przetwarzanych w Urzędzie,
8) **Dostępności danych** - należy przez to rozumieć właściwość danych polegającą na tym, że są one dostępne i mogą być wykorzystywane na żądanie uprawnionej osoby, podmiotu lub procesu,
9) **Ewaluacji ryzyka** - należy przez to rozumieć proces porównywania wyników **analizy ryzyka** z **kryteriami ryzyka** w celu stwierdzenia, czy **ryzyko** (jego wielkość) jest akceptowalne lub tolerowane,
10) **Identyfikacji ryzyka** – należy przez to rozumieć wyszukanie, rozpoznanie i opisanie rodzajów ryzyk, związanych z zachowaniem poufności, dostępności i integralności informacji przetwarzanych w Urzędzie,

11) **Incydencie bezpieczeństwa** – należy przez to rozumieć pojedyncze niepożądane lub niespodziewane zdarzenie wskazujące na potencjalne naruszenie bezpieczeństwa, błąd mechanizmu kontrolnego lub uprzednio nieznaną sytuację, która może być istotna z perspektywy bezpieczeństwa, w przypadku których występuje znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji

12) **Integralności danych** – należy przez to rozumieć właściwość danych stanowiącą o ich dokładności i kompletności,

13) **Kryteriach ryzyka -** należy przez to rozumieć poziomy odniesienia, względem

14) **Mechanizmach kontroli** - należy przez to rozumieć wszystkie działania i procedury podejmowane lub ustanawiane dla zachowania poufności, dostępności i integralności informacji przetwarzanych w Urzędzie:

   a) Środki (Zabezpieczenia) organizacyjne
   b) Środki (Zabezpieczenia) techniczne
   c) dokumentację systemu zarządzania bezpieczeństwem informacji (polityka bezpieczeństwa, zarządzenia, procedury, instrukcje, oświadczenia i zobowiązania)
   d) dokumentowanie poszczególnych zdarzeń,
   e) podział obowiązków,
   f) nadzór,
   g) rejestrowanie zdarzeń (incydentów/naruszeń) bezpieczeństwa informacji,
   h) ograniczenie dostępu do zasobów (aktywów) informacyjnych,

15) **Ocenie ryzyka -** należy przez to rozumieć całościowy proces **identyfikacji ryzyka, analizy ryzyka** oraz **ewaluacji ryzyka** przez punktową ocenę prawdopodobieństwa wystąpienia zdarzenia i wielkości skutku wystąpienia (wpływu/konsekwencji) umożliwiająca hierarchizację zidentyfikowanego ryzyka,

16) **Planie zarządzania ryzykiem (Planie postępowania z ryzykiem) -** należy przez to rozumieć plan określający podejście, elementy zarządzania i zasoby, które będą zastosowane w zarządzaniu **ryzykiem,**

17) **Podatności** – należy przez to rozumieć słabość zasobu lub mechanizmu kontrolnego, która może być wykorzystana przez zagrożenie

18) **Postępowaniu z ryzykiem (działaniach zaradczych)-** należy przez to rozumieć proces modyfikacji **ryzyka,**

   a. Postępowanie z ryzykiem może uwzględniać:
      i. – usunięcie **źródła ryzyka**;

ii. – zmianę **prawdopodobieństwa**;

iii. – zmianę **następstw;**

iv. – dzielenie ryzyka wraz z inną stroną lub stronami (łącznie z umowami i finansowaniem ryzyka); – unikanie ryzyka poprzez decyzję o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko;

v. – retencję ryzyka na podstawie świadomej decyzji

vi. – podjęcie ryzyka w celu wykorzystania szansy.

19) **Poufności danych** - należy przez to rozumieć właściwość danych polegająca na tym, że pozostają one niedostępne lub niejawne dla nieuprawnionych osób, podmiotów lub procesów,

20) **Poziomie ryzyka** - należy przez to rozumieć wielkość **ryzyka** lub kombinacji ryzyk, wyrażona w postaci kombinacji **następstw** oraz ich **prawdopodobieństwa** (Ryzyko jest mierzone wpływem (siłą oddziaływania) oraz prawdopodobieństwem jego wystąpienia),

21) **Prawdopodobieństwie** ziszczenia się ryzyka - należy przez to rozumieć częstotliwość występowania zdarzenia objętego ryzykiem,

22) **Ryzyku** – należy przez to rozumieć możliwość wystąpienia dowolnego zdarzenia, działania lub zaniechania (braku działania), którego skutkiem może być utrata poufności, dostępności i integralności informacji, szkoda w majątku lub wizerunku urzędu lub utrata szansy poprzez niewykorzystanie wszystkich możliwości (osiągnięcie mniej niż to było możliwe). Ryzyko jest konsekwencją występowania niepewności co do kształtowania się przyszłości,

23) **Ryzyku rezydualnym (szczątkowym)** - należy przez to rozumieć **ryzyko** pozostające po zastosowaniu działań określonych w **postępowaniu z ryzykiem,**

24) **Właścicielu ryzyka** – należy przez to zrozumieć Kierującego komórką organizacyjną, będącą posiadaczem Aktywu informacyjnego,

25) **Wpływie ryzyka (następstwie)** – należy przez to rozumieć skutki (konsekwencje) finansowe, organizacyjne, prawne, społeczne czy wizerunkowe dla Urzędu spowodowane przez zdarzenie objęte ryzykiem,

26) **Ustalaniu kontekstu** - należy przez to rozumieć definiowanie zewnętrznych i wewnętrznych parametrów, które powinny być uwzględniane podczas zarządzania ryzykiem,

27) **Zagrożeniu** – należy przez to rozumieć potencjalną przyczynę niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji

28) **Zarządzaniu ryzykiem** - należy przez to rozumieć proces identyfikacji, oceny i przeciwdziałania ryzyku; proces ten obejmuje także monitorowanie ryzyka i środków podejmowanych w celu jego ograniczenia,

29) **Zdarzeniu** - należy przez to rozumieć wystąpienie lub zmiana konkretnego zestawu okoliczności,

3. Celem zarządzania ryzykiem jest w szczególności:

- określenie trybu i zasad przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy
- zapewnienie odpowiednich mechanizmów kontroli, w tym środków (zabezpieczeń) organizacyjnych i technicznych i ich stałej adekwatności w odniesieniu do **kontekstu** wewnętrznego i zewnętrznego Urzędu
- usprawnienie procesu planowania
- tam gdzie to możliwe, zapewnienie kierownictwu Urzędu wczesnej informacji o zagrożeniach dla integralności, dostępności lub poufności informacji

4. Zarządzanie ryzykiem odbywa się według zasad:

- Integracji z procesem zarządzania.
- Powiązania z celami i zadaniami Urzędu,
- Przypisania odpowiedzialności,
- Proporcjonalności działań przeciwdziałających ryzyku do poziomu ryzyka.
- Integracji z systemem zarządzania.

5. Proces zarządzania ryzykiem obejmuje:

- Identyfikację i analizę ryzyka w odniesieniu do określonych aktywów informacji
- Ustalenie akceptowalnego poziomu ryzyka.
- Ustalenie metody przeciwdziałania ryzyku.
- Przeciwdziałanie ryzyku,
- Monitorowanie procesu i dokonywanie zmian,
- Ocenę skuteczności podjętych działań i dokonywanie ewentualnych zmian prowadzących do efektywnego zapewnienia integralności, dostępności lub poufności informacji

6.1. W terminie do 31 marca każdego roku kalendarzowego Kierownicy komórek organizacyjnych (przy udziale Administratora Bezpieczeństwa Informacji) wypełniają i przekazują do Administratora Bezpieczeństwa Informacji formularz „Identyfikacja i ocena ryzyka" będący **załącznikiem nr 1** do niniejszej procedury .

2. Kierownicy komórek organizacyjnych powinni włączać podległych pracowników w proces identyfikacji, analizy i ustalania metod przeciwdziałania ryzyku.

3. Administrator Bezpieczeństwa Informacji zobowiązany jest do koordynacji działań podejmowanych przez Kierowników komórek organizacyjnych w ramach procesu zarządzania ryzykiem bezpieczeństwa informacji.

7.1. **Ocena ryzyka** – jest to proces, w którym identyfikuje się ryzyko i dokonuje jego oceny pod kątem prawdopodobieństwa wystąpienia danego ryzyka i możliwych jego skutków. Należy określić akceptowalny poziom ryzyka. Identyfikację i ocenę ryzyka oraz ustalenie metod przeciwdziałania wykonują Kierownicy komórek organizacyjnych.

2. W procesie oceny ryzyka można wyróżnić trzy etapy:

1) identyfikacja ryzyka

2) analiza (pomiar) ryzyka

3) ewaluacja (hierarchizacja) ryzyka

8.1. **Identyfikacja i analiza ryzyka** - odbywa się w oparciu analizę ryzyk w odniesieniu do aktywów informacyjnych Urzędu - ryzyko ustala się dla każdego z aktywów informacyjnych.

2. Kierownicy dokonując identyfikacji i analizy ryzyka biorą pod uwagę incydenty bezpieczeństwa informacji jakie wcześniej miały miejsce w urzędzie,

3. Dla każdego aktywu informacyjnego Kierownicy określają trzy wartości:

a) PRAWDOPODOBIEŃSTWA <u>pierwotnego</u>

tj. utraty poufności/dostępności i/lub integralności danej informacji:

1 (niskie) - Nie więcej niż 10% / Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem nie zdarzy się w ciągu roku,

2 (średnie) 10 – 40% / Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz w ciągu roku,

3 (wysokie) 40-75% / Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się kilkakrotnie w ciągu roku,

4 (bardzo wysokie) zdarzenie niemal pewne / Istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku,

b) SKUTKU (WPŁYW ryzyka; następstwa; konsekwencje) w tym:

1. skutek finansowy

jaki może wystąpić w przypadku utraty poufności/dostępności i/lub integralności informacji:

Punktacja Opis

4 (bardzo wysoki) Strata finansowa powyżej 1 mln. zł

3 (wysoki) Strata finansowa od 100 tys.– 1 mln. zł

2 (średni) Strata finansowa od 3 tys.– 100 tys. zł

1 (niski) Strata finansowa nie większa niż 3 tys. zł

2. skutek wizerunkowy (wpływ na reputację urzędu)

jaki może wystąpić w następstwie utraty poufności/dostępności i/lub integralności informacji:

4 (bardzo wysoki) Utrata reputacji w mediach ogólnopolskich

3 (wysoki) Utrata reputacji w mediach lokalnych

2 (średni) Utrata reputacji u zainteresowanych stron

1 (niski) Brak utraty reputacji

3. wpływ na realizację celów urzędu

4 (bardzo wysoki) - zdarzenie objęte ryzykiem powoduje uszczerbek mający **krytyczny** wpływ na realizację kluczowych zadań albo osiąganie założonych celów

3 (wysoki) zdarzenie objęte ryzykiem powoduje uszczerbek mający **duży** wpływ na realizację kluczowych zadań albo osiąganie założonych celów

2 (średni) Zdarzenie objęte ryzykiem ma negatywny wpływ na efektywność działania i jakość wykonywanych zadań. Z wystąpieniem zdarzenia objętego ryzykiem może się wiązać trudny proces przywracania stanu poprzedniego.

1 (niski) Zdarzenie objęte ryzykiem powoduje zakłócenie lub opóźnienie w wykonywaniu zadań. Nie wpływa osiąganie celów i jakość wykonywanych zadań. Skutki zdarzenia można łatwo usunąć.

c) SKUTECZNOŚCI stosowanych „MECHANIZMÓW KONTROLI"

Analiza ryzyka obejmuje także identyfikację i ocenę adekwatności funkcjonujących w Urzędzie mechanizmów kontrolnych, których zadaniem jest przeciwdziałanie i minimalizacja ryzyka w odniesieniu do bezpieczeństwa informacji - punktowa **ocena skuteczności** (współczynnik korygujący) jest następująca

UWAGA – odwrotność oceny !!! – najlepsze zabezpieczenie ma wartość 1

1 (bardzo wysoka) najnowocześniejsze w swojej klasie,

2 (wysoka) wdrożone mechanizmy kontroli/zabezpieczenia są sprawdzone i/lub posiadają niezależnie potwierdzoną skuteczność (np. sejf o określoną klasą odporności)

3 (średnia) występują częściowe mechanizmy kontroli/zabezpieczenia, które chronią tylko wybrane obszary

4 (niska) np. **brak** zabezpieczeń lub zabezpieczenia nie spełniają wymagań minimalnych określonych w odrębnych dokumentach (np. wymaganiach i zaleceniach bezpieczeństwa SRP)

9. Poziom (wartość) ryzyka

Poziom danego ryzyka to ILOCZYN

- prawdopodobieństwa
- **najwyższego z określonych** skutków *(przykład: jeżeli „skutek finansowy"=2, „wizerunkowy"=1, a „wpływ na realizację celów urzędu"=3 – wynikiem będzie 3)*
- oceny skuteczności „mechanizmów kontroli"

10. Ewaluacji ryzyka – to porównywanie wyników **analizy ryzyka** z **kryteriami ryzyka:**

<16 oznacza **RYZYKO <u>NIEZNACZNE</u> Akceptowalne**, tzw. „ryzyko pomijalne", podlegające ponownej ocenie tylko na wniosek uczestnika procesu analizy ryzyka lub podlegające ocenie podczas nowego cyklu analizy ryzyka

17-32 oznacza **RYZYKO <u>UMIARKOWANE</u> Tolerowane** ze szczególnym uwzględnieniem procesu monitorowania procesu

33-64 oznacza **RYZYKO <u>POWAŻNE</u> - Nieakceptowalne**, wymagające wdrożenia i oceny skuteczności rozwiązań minimalizujących ryzyko

11.1. **Postępowanie z ryzykiem -** to podejmowanie działań mających na celu sprowadzenie ryzyka do poziomu możliwie niskiego.

2. w przypadku ryzyka **NIEZNACZNEGO**:

2.1.ponowna ocena ryzyka odbywa się tylko na wniosek właściciela ryzyka lub podczas nowego cyklu analizy ryzyka,

3. w przypadku ryzyka **UMIARKOWANEGO**:

3.1.właściciel ryzyka na bieżąco monitoruje ryzyko tak, aby nie dopuścić do wzrostu do poziomu nieakceptowanego,

3.2.właściciel ryzyka na bieżąco podejmuje decyzje mające na celu obniżenie ryzyka do poziomu niższego (w przypadku stwierdzenia takiego stanu należy uzupełnić formularz „Identyfikacja i ocena ryzyka" będący **załącznikiem nr 1** do niniejszej procedury i przekazać go ponownie do Administratora Bezpieczeństwa Informacji),

3.3. w przypadku wzrostu ryzyka do poziomu nieakceptowanego, właściciel ryzyka niezwłocznie informuje o tym fakcie Administratora Bezpieczeństwa Informacji, w celu podjęcia działań mających na celu zminimalizowanie ryzyka.

4. w przypadku ryzyka **POWAŻNEGO:**

4.1 właściciel ryzyka o fakcie pojawienia się ryzyka „Nieakceptowalnego" informuje Administratora Bezpieczeństwa Informacji w celu podjęcia działań mających na celu zminimalizowanie ryzyka

4.2 w stosunku do ryzyk **Nieakceptowalnych** właściciel ryzyka (**kierownik**) proponuje **działania zaradcze**

12.1. Wypełniony formularz „Identyfikacja i ocena ryzyka" będący **załącznikiem nr 1** do niniejszej procedury przekazywany jest do 31 marca każdego roku kalendarzowego do Administratora Bezpieczeństwa Informacji w ramach sprawozdań z realizacji zadań.

2. W przypadku „ryzyka **poważnego**" kierownicy wraz z formularzem przekazują notatkę/e-mail z propozycjami działań zaradczych

3. Proces analizy ryzykiem podlega całościowej identyfikacji wszystkich ryzyk i ich ocenie **co najmniej raz w roku**. Wyniki z oceny stanowią dane wejściowe do Przeglądu Zarządzania w ramach istniejącego systemu zarządzania jakością.

4. Administrator Bezpieczeństwa Informacji wpisuje do **„PLANU ZARZĄDZANIA RYZYKIEM",** będącego **załącznikiem nr 2,** wszystkie ryzyka nieakceptowalne oraz propozycje postępowania z ryzykiem (sugerowane przez kierowników oraz własne).

13.1. Propozycję Planu zarządzania ryzykiem będącego **załącznikiem nr 2** przedkłada do zatwierdzenia **Burmistrzowi**

2. Na Przeglądzie Zarządzania **Burmistrz** dokonuje przeglądu ryzyk i akceptuje bądź nie propozycje postępowania z ryzykiem zaproponowane przez Kierowników.

3. Zatwierdzony Plan zarządzania ryzykiem będący **załącznikiem nr 2** podaje się do wiadomości pracowników których plan ten dotyczy

4. Za terminowe podjęcie działań zaradczych odpowiada właściciel ryzyka (gestor)

5. Wykonanie zadań związanych z realizacją planu zarządzania ryzykiem jest zgłaszane za pośrednictwem poczty e-mail do Administratora Bezpieczeństwa Informacji

6. Administratora Bezpieczeństwa Informacji dokonuje ponownej **Analizy ryzyka** „rezydualnego" („szczątkowego"), w odniesieniu do którego plan był realizowany, w celu sprawdzenia czy ryzyko osiągnęło poziom „**nieznaczne**" lub „**umiarkowane**";

7. Jeżeli pomimo realizacji planu zarządzania z ryzykiem (postępowania z ryzykiem) ryzyko pozostaje na poziomie „**poważne**" należy opracować nowy plan zarządzania ryzykiem lub po uwzględnieniu okoliczności (np. wymaganych nakładów finansowych) podjąć decyzję o jego **tolerowaniu**;

8. Tylko i wyłącznie **Burmistrz** może dokonać akceptacji „ryzyka rezydualnego" na poziomie „**Poważnym - Nieakceptowalnym**"

9. Po wystąpieniu incydentu Administrator Bezpieczeństwa Informacji decyduje czy potrzebna jest poza planowa ocena ryzyka bezpieczeństwa informacji w obszarze zasobów, osób lub procesów których dotyczył incydent.

BURMISTRZ
mgr inż. Antoni Kopeć

Załącznik nr 1 - Identyfikacja i ocena ryzyka utraty poufności, dostępności i integralności SZBI

AKTYWO INFORMACJI	ZAGROŻENIE	poziom prawdopodobieństwa pierwotnego*	skutek finansowy*	skutek wizerunkowy*	Wpływ na realizację celów urzędu*	MAX [4 lub 5 lub 6]	Stosowanie poszczególnych zabezpieczeń ^/^^	ocena skuteczności zabezpieczeń	Poziom RYZYKA [3x7x9]	KATEGORIA (OCENA)
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]

* SKALA OCEN: 4 (bardzo wysokie); 3 (wysokie); 2 (średnie); 1 (niskie) – szczegóły zobacz procedura

^ zabezpieczenia minimalne SRP (oznacz po wpisaniu)

^^ zabezpieczenia zalecane SRP (oznacz po wpisaniu)

Data: .....

Opracował: .....

Załącznik nr 2 – Plan zarządzania ryzykiem / Cele bezpieczeństwa informacji

Lp.	RYZYKO / CEL bezpieczeństwa informacji	Zadania do wykonania i zasoby jakie będą potrzebne	Odpowiedzialny za realizację	Planowany termin	Opis wykonania/ data / OCENA
[1]	*[2]*	*[3]*	*[4]*	*[5]*	*[6]*
1					
2					
3					
4					
5					

Data: .....

Zatwierdził: .....