**Zarządzenie nr 108/2015**
**Burmistrza Miasta Radymna**
**z dnia 14 grudnia 2015 roku**

**w sprawie wdrożenia Polityki Bezpieczeństwa Informacji w Urzędzie Miasta Radymna**

Na podstawie § 5 ust. 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz. U. nr 93 poz. 545) oraz w związku z art. 31 i art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. (tekst jednolity Dz. U. z 2015 r. poz. 1515 z późniejszymi zmianami) zarządza się, co następuje:

§ 1

Wprowadza się do użytku "Politykę Bezpieczeństwa Informacji", stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2

Wykonanie Zarządzenia powierza się Sekretarzowi Miasta Radymna.

§ 3

Nadzór nad przestrzeganiem Polityki Bezpieczeństwa Informacji powierza się Informatykowi, wykonującemu czynności Administratora Bezpieczeństwa Informacji w Urzędzie Miasta Radymna.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz
Miasta Radymna
***Krzysztof Roman***

Załącznik Nr 1
Do Zarządzenia nr 106/2015
Burmistrza Miasta Radymna
z dnia 08 grudnia 2015 roku

# POLITYKA BEZPIECZEŃSTWA INFORMACJI

## 1. Wstęp

O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągania zamierzonego celu. W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją.

Informacja jest jednym z najważniejszych zasobów Urzędu, dlatego powinna być chroniona na każdym szczeblu organizacji.

Najwyższe kierownictwo Urzędu zobowiązuje się do podejmowania niezbędnych działań mających na celu zapewnienie ochrony informacji na pożądanym poziomie, a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informacyjnych.

## 2. Definicje:

1. **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji.
2. **Ryzyko** – prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.
3. **Szacowanie ryzyka** – całościowy proces analizy i oceny ryzyka.
4. **Aktyw/zasób** – wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania).
5. **Poufność** – zapewnienie dostępu do informacji tylko osobom upoważnionym.
6. **Integralność** – zapewnienie dostępu do informacji tylko osobom upoważnionym.
7. **Dostępność** – zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy gdy jest to uzasadnione.
8. **Postępowanie z ryzykiem** – proces wyboru i wdrażania środków modyfikujących ryzyko.
9. **Zarządzanie ryzykiem** – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.
10. **Zdarzenie związane z bezpieczeństwem informacji** – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
11. **Incydent związany z bezpieczeństwem informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
12. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
13. **Urząd** – Urząd Miasta Radymna.

## 3. Zakres Systemu Bezpieczeństwa Informacji

System Zarządzania Bezpieczeństwa Informacji (SZBI) w Urzędzie odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. Elementy SZBI zostały opracowane, wdrożone i są utrzymywane w oparciu o normę PN-ISO/IEC 27001:2007. Zakres SZBI dotyczy obsługi administracyjnej ludności i podmiotów gospodarczych.

Zakresy określone przez dokument Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Urzędu, w szczególności do:

1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
2. informacji będących własnością Urzędu;
3. informacji będących własnością klientów Urzędu, uzyskanych na podstawie zawartych umów;
4. wszystkich lokalizacji Urzędu, czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
5. wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

## 4. Deklaracja Kierownictwa w zakresie bezpieczeństwa informacji w Urzędzie

**Najwyższe kierownictwo Urzędu, stojąc na stanowisku, że informacja jest newralgicznym zasobem każdej organizacji, wdrożyło system zarządzania bezpieczeństwem informacji.**

**Priorytetowym celem systemu jest spełnienie wymagań prawnych oraz zapewnienie ciągłości działania organizacji, poufności danych wrażliwych i dostępności wymaganych informacji.**

**Przez bezpieczeństwo informacji w Urzędzie rozumie się zapewnienie dostępności, zabezpieczenie przed nieuprawnionym dostępem, naruszeniem integralności bądź zniszczeniem aktywów związanych z przechowywaniem i przetwarzaniem informacji.**

**Zakres ochrony i podjęte środki są adekwatne do własności aktywów związanych z systemami przetwarzania informacji.**

**Główne cele stawiane przed systemem zarządzania bezpieczeństwem informacji:**

1. **zapewnienie spełnienia wymagań prawnych,**
2. **ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem,**
3. **podnoszenie świadomości pracowników,**
4. **zmniejszenie ryzyka utraty informacji,**
5. **zaangażowanie wszystkich pracowników w ochronę informacji.**

**W Urzędzie zapewniamy bezpieczeństwo informacji poprzez:**

1. **zarządzanie ryzykiem, na które składają się identyfikacja prawdopodobieństwa wystąpienia zagrożenia oraz ich następstw (skutków) wraz z określeniem i wdrożeniem działań zabezpieczających zasoby.**

**Kierownictwo Urzędu zapewnia środki niezbędne do realizacji Polityki Bezpieczeństwa Informacji.**

## 5. Organizacja bezpieczeństwa informacji w Urzędzie

Odpowiedzialność za bezpieczeństwo informacji w Urzędzie ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Najwyższe Kierownictwo odpowiedzialne jest za zapewnienie zasobów niezbędnych dla funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń. Wydaje zgodę na użytkowanie urządzeń służących do przetwarzania informacji i zabezpieczeń. Decyduje również o współpracy w zakresie bezpieczeństwa z innymi podmiotami.

Każdy pracownik Urzędu jest zapoznawany z zasadami bezpieczeństwa w swojej komórce organizacyjnej wynikającymi z postanowień niniejszego zarządzenia.

Stażyści oraz praktykanci również są zapoznawani z tymi zasadami. Kierownik komórki organizacyjnej jest odpowiedzialny za ochronę bezpieczeństwa informacji w Referacie / Wydziale, a w szczególności za monitorowanie integralności i dostępności posiadanych zasobów informacji, nadzorowanie przestrzegania zasad bezpieczeństwa przez podległych pracowników oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa. Właściciel aktywa odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.

### 5.1 Dokumentacja systemu zarządzania bezpieczeństwem informacji

Dokumentacja systemu zarządzania bezpieczeństwem składa się z dwóch głównych elementów. Są nimi:

- Polityka Bezpieczeństwa Informacji w Urzędzie;
- Arkusz analizy ryzyka wraz z planem postępowania z ryzykiem zawierającym cele bezpieczeństwa informacji.

### 5.2. Polityka kontroli dostępu do informacji

Dostęp do informacji przechowywanych i przetwarzanych w Urzędzie jest poddany kontroli wynikającej z obowiązujących przepisów prawa powszechnego oraz dodatkowych wymagań bezpieczeństwa, przyjętych w normie PN-ISO/IEC 27001:2007. Kontrola polega na:

1. wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
2. zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny;
3. stosowaniu bezpiecznych systemów przetwarzania informacji;
4. bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

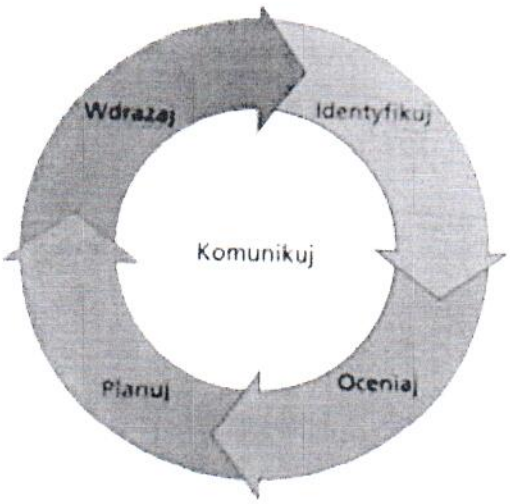
## 6. Zarządzanie aktywami i ryzykami

Urząd zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne zgodnie z formularzem załącznika Nr 1 do niniejszej Polityki. Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem (wyznaczania celów bezpieczeństwa informacji). Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Urzędu. Poziom ryzyka określa się na podstawie załącznika Nr 2 do niniejszej Polityki.

Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego. Przyjmuje się, że w danym okresie wyznacza się plan zarządzania ryzykiem dla ryzyk, których wartość jest najwyższa. Za okres przyjmuje się rok kalendarzowy.

Ryzyka są przeglądane i aktualizowane co najmniej raz w roku oraz po zmianach mających wpływ na system bezpieczeństwa informacji. Plany postępowania z ryzykiem dokumentuje się w oparciu o załącznik Nr 3 do niniejszej Polityki.

W Urzędzie stosuje się procedurę zarządzania ryzykiem zalecaną przez metodologię PRINCE2 obejmującą pięć następujących kroków: 1. Identyfikuj 2. Oceniaj 3. Planuj 4. Wdrażaj 5. Komunikuj.




Rys. Procedura zarządzania ryzykiem

Identyfikowanie ryzyk polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji. W tym celu przyjęto jako podstawową technikę mieszaną, będącą połączeniem technik „przeglądu doświadczeń" oraz „burzy mózgów". Przegląd doświadczeń opiera się na wiedzy eksperckiej oraz analizie wcześniejszych incydentów związanych z naruszeniem bezpieczeństwa informacji.
Burza mózgów opiera się na myśleniu grupowym, które może być bardziej produktywne niż indywidualne oraz umożliwia zrozumienie poglądów innych interesariuszy na temat zidentyfikowanych ryzyk.

Ocenianie polega na oszacowaniu zagrożeń oraz możliwości ich zmaterializowania w przypadku nie podjęcia odpowiednich działań. Do tego celu wykorzystano „macierz prawdopodobieństwo/wpływ". Zawiera ona wartości niezbędne do sklasyfikowania zagrożeń w ujęciu jakościowym. Skale prawdopodobieństwa są miarami pochodzącymi z wartości procentowych, natomiast skale wpływu są wybrane w celu określenia miary oddziaływania na Urząd.

Planowanie polega na przygotowaniu określonych reakcji zarządczych w celu usunięcia lub zmniejszenia zagrożeń wynikających ze zmaterializowania się określonego ryzyka. Wprowadza się następujące możliwe reakcje na ryzyko:

1. Unikanie (prewencja) - jeżeli to możliwe podjęcie stosownych reakcji zarządczych tak aby zagrożenie (przypisane do danego ryzyka) nie mogło wpłynąć na bezpieczeństwo informacji lub nie mogło zaistnieć.
2. Redukowanie - działania podjęte w celu zmniejszenia prawdopodobieństwa wystąpienia zdarzenia lub ograniczenia jego wpływu (redukcja jednego lub dwóch parametrów z macierzy prawdopodobieństwo/wpływ).
3. Plan rezerwowy - opracowanie działań, które zostaną podjęte w celu zredukowania skutków zagrożenia dla ryzyka, które się zmaterializowało.

Wdrażanie polega na zapewnieniu, aby planowane reakcje na ryzyko zostały zrealizowane oraz aby podjęte zostały działania korygujące w przypadku gdyby reakcje te nie spełniły związanych z nimi oczekiwań. Istotnym elementem ról i obowiązków w zarządzaniu ryzykiem. Wprowadza się następujące role:

1. Właściciela ryzyka - wskazane stanowisko lub osoba odpowiedzialna zarządzanie, monitorowanie i kontrolowanie wszystkich aspektów przypisanego jej ryzyka łącznie z wdrożeniem wybranych reakcji na zagrożenie.
2. Wykonawca reakcji na ryzyko - stanowisko lub osoba wyznaczona do wykonywania działań związanych z reakcją na konkretne ryzyko. Wykonawca reakcji wspiera właściciela ryzyka i otrzymuje od niego polecenia.

Komunikacja polega na zapewnieniu, aby wszystkie informacje o zagrożeniach docierały do wszystkich zainteresowanych. Jako podstawową formę komunikacji wprowadza się w Urzędzie drogę elektroniczną poprzez pocztę email.

## 7. Zarządzanie systemami i sieciami

Urząd dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych. Skuteczna realizacja postawionego celu możliwa jest dzięki:

1. kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi;
2. kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,
3. prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach w celu zapewnienia bezpieczeństwa systemów produkcyjnych;

4. nadzorowaniu usług dostarczanych przez strony trzecie, w szczególności odbieraniu ich i akceptowaniu w sposób świadomy uwzględniający jego wpływ na istniejący system bezpieczeństwa;
5. wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym i mobilnym;
6. systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;
7. bieżącym monitorowaniu aktywów informacyjnych

## 8. Bezpieczeństwo zasobów ludzkich

Urząd zapewnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonej procedurze rozwiązywania umów o pracę.

## 9. Bezpieczeństwo fizyczne, sprzętu i okablowania, konfiguracji i eksploatacji sieci

W Urzędzie określono następujące kierunkowe standardy:

- standard bezpieczeństwa fizycznego;
- standard bezpieczeństwa sprzętu i okablowania;
- standard konfiguracji i eksploatacji sieci.

Z uwagi na to, że standardy zawierają informacje, których ujawnienie nieuprawnionym stronom trzecim mogłoby w istotnym stopniu obniżyć poziom bezpieczeństwa informacji, są udostępnione tylko pracownikom Urzędu wykonującym zadania określone w standardach.
Przedmiot poszczególnych standardów:

1. standard bezpieczeństwa fizycznego: perymetr bezpieczeństwa fizycznego, kontrola fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych, obszary ogólnie dostępne;
2. standard bezpieczeństwa sprzętu i okablowania: rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem organizacji, bezpieczne usuwanie sprzętu, wynoszenie majątku;
3. standard konfiguracji i eksploatacji sieci: środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, Przesyłanie wiadomości drogą elektroniczną, Polityka korzystania z usług sieciowych, identyfikacja sprzętu w sieciach, ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń sieci, routing, nadzorowanie słabości technicznych.

## 10. Zgodność z wymaganiami prawnymi i innymi

Urząd dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych

standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawnych, zobowiązań wynikających z ustaw, zarządzeń lub umów oraz wymagań bezpieczeństwa.

Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji.

## 11. Postanowienia końcowe

Urząd wymaga zapoznania się pracowników z dokumentem Polityki Bezpieczeństwa Informacji. Za złożenie przez nich stosownych oświadczeń o zapoznaniu się odpowiada kierownik każdej komórki organizacyjnej Urzędu. Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami operacyjnymi) powoduje skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez sąd.

Załącznik Nr 1
do Polityki Bezpieczeństwa Informacji
w Urzędzie Miasta Radymna

**Identyfikacja i ocena ryzyk bezpieczeństwa informacji**

| Lp | Zdarzenie | Obecnie stosowane zabezpieczenia | P | W | R |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Załącznik Nr 2
do Polityki Bezpieczeństwa Informacji
w Urzędzie Miasta Radymna

## Matryca analiza ryzyka

| Prawdopodobieństwo | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 0.9 | B. wysokie 71-90% | 0.045 | 0.09 | 0.18 | 0.36 | 0.72 |
| | 0.7 | Wysokie 51-70% | 0.035 | 0.07 | 0.14 | 0.28 | 0.56 **ID:2** |
| | 0.5 | Średnie 31-50% | 0.025 | 0.05 | 0.10 **ID:7,10** | 0.20 | 0.40 |
| | 0.3 | Niskie 11-30% | 0.015 | 0.03 **ID:6** | 0.06 **ID:3** | 0.12 | 0.24 **ID:1,4,12** |
| | 0.1 | B. niskie <10% | 0.005 | 0.01 **ID:5** | 0.02 **ID:8,9,11** | 0.04 | 0.08 |
| | | | B. mały | Mały | Średni | Duży | B. duży |
| | | | 0.05 | 0.1 | 0.2 | 0.4 | 0.8 |
| | | | **Wpływ** | | | | |

Załącznik Nr 3
do Polityki Bezpieczeństwa Informacji
w Urzędzie Miasta Radymna

**Plan postępowania z ryzykiem**

| Reakcja | Działanie | Właściciel ryzyka | Wykonawca reakcji na ryzyko | Termin |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |