BURMISTRZ
Gminy Żmigród

# ZARZĄDZENIE Nr 0050.159.2015
## BURMISTRZA GMINY ŻMIGRODZIE
## z dnia 30 października 2015 roku

**w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miejskim w Żmigrodzie**

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2015 r. poz. 1515 ze zm.), art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 ze zm.), zarządzam co następuje:

§ 1. 1. Wyznaczam Panią Joannę Monastyrską na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Miejskim w Żmigrodzie. Zakres działania ABI stanowi załącznik Nr 1 do niniejszego zarządzenia.

2. Wyznaczam Pana Zeyada Balloura na Administratora Systemów Informatycznych (ASI) w Urzędzie Miejskim w Żmigrodzie. Zakres działania ASI stanowi załącznik Nr 2 do niniejszego zarządzenia.

§ 2. Traci moc § 3 Zarządzenia Burmistrza Gminy Żmigród Nr 0152/52/2009 z dnia 28 października 2009 r. w sprawie Polityki Bezpieczeństwa w Urzędzie Miejskim w Żmigrodzie.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

mgr inż. Robert Lewandowski

| L.p. | Imię i Nazwisko | Zakres kompetencji | Data i podpis | Uwagi |
|---|---|---|---|---|
| 1. | Joanna Monastyrska / Sekretarz Gminy | Przygotował/przegląd | 30.10.2015 | |
| 2. | Karolina Kaszuba / Radca Prawny | Opinia | 30.10.2015 | |
| 3. | Anna Dobrowolska / Skarbnik Gminy lub osoba upoważniona | Opinia | | |
| 4. | Grażyna Kalicka / Pełnomocnik ds. SZJ | Przegląd | 30.10.2015 | |

Załącznik Nr 1 do
Zarządzenia Nr 0050.159.2015
Burmistrza Gminy Żmigród
z dnia 30 października 2015 r.

## Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

**Do zadań Administratora Bezpieczeństwa Informacji należy:**

Stosowanie środków organizacyjnych i technicznych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2. Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
3. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób.
4. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisywane są dane osobowe.
5. Nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających częstotliwość ich zmiany.
6. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych.
7. Nadzór nad wykonywaniem kopii awaryjnych.
8. Nadzór nad systemem komunikacji w sieci komputerowej.
9. Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
10. Kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane).
11. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń.
12. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe.
13. Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.
14. Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.

Załącznik Nr 2 do
Zarządzenia Nr 0050.159.2015
Burmistrza Gminy Żmigród
z dnia 30 października 2015 r.

## Zakres działania Administratora Systemu Informatycznego (ASI)

Administrator Systemu Informatycznego, w zakresie zadań wykonywanych dla zapewnienia systemom bezpieczeństwa, zgodnego z celami i metodologią wdrożonej polityki bezpieczeństwa informacji, współpracuje bezpośrednio z Administratorem Bezpieczeństwa Informacji (ABI).

**Do zadań Administratora Systemu Informatycznego należy:**

1. Formułowanie, w uzgodnieniu z administratorem danych i/lub osobami, do których administrator delegował zarządzanie uprawnieniami oraz ABI, sposobu określania uprawnień w systemach informatycznych.
2. Realizacja decyzji Administratora Danych Osobowych odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu tj.:
   1) tworzenie kont użytkowników w systemach informatycznych,
   2) przypisywanie, do kont, startowych haseł uwierzytelniających użytkowników tych kont,
   3) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
   4) resetowanie utraconych haseł,
   5) usuwanie kont i uprawnień dla kont osób które zakończyły pracę w Urzędzie,
   6) dostarczanie ABI informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych.
3. Planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie Gminy.
4. Planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych.
5. Automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych.
6. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
7. Monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników.
8. Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
9. Zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych.
10. Systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego.
11. Zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki.
12. Rozwiązywanie, samodzielnie i we współpracy z pozostałym personelem IT, problemów towarzyszących eksploatacji systemów informatycznych.
13. Przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji.
14. Prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT.