**ZARZĄDZENIE Nr 0050.55.2015**

**Burmistrza Miasta i Gminy Suchedniów**

**z dnia 30 czerwca 2015r.**

**w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miasta i Gminy w Suchedniowie**

Na podstawie art. 31 oraz art. 33 ustawy z dnia 8 marca 1990r.   
o samorządzie gminnym (tj. Dz. U. z 2013r. poz. 594 ze zm.) w związku z art. 36a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2014r. poz. 1182 ze zm.) zarządzam co następuje:

**§ 1.**

W celu zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych osobowych przed ich udostepnieniem osobom nieuprawnionym, zabraniem przez osobę nieupoważnioną, przetworzeniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem – powołuję na **Administratora Bezpieczeństwa** **Informacji** w Urzędzie Miasta i Gminy w Suchedniowie, zwaną dalej **ABI** –

**Panią Beatę Borkowską.**

**§ 2.**

1. Ustala się ramowy zakres działania ABI zgodnie z załącznikiem Nr 1 do nin. zarządzenia.
2. Szczegółowe zadania ABI określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityka bezpieczeństwa.

**§ 3.**

Wyznaczam **Pana Łukasza Osucha** na **Administratora Systemów Informatycznych**, zwanego dalej **ASI** w Urzędzie Miasta i Gminy w Suchedniowie.

**§ 4.**

1. Ustala się ramowy zakres działania ASI zgodnie z zał. Nr 2 do nin. Zarządzenia.
2. Szczegółowe zadania ASI określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityka bezpieczeństwa.

**§ 5.**

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy

Cezary Błach

Zał. Nr 1

do Zarządzenia Nr 0050.55.2015

Burmistrza Miasta i Gminy Suchedniów

z dnia 30 czerwca 2015r.

**Zakres działania Administratora Bezpieczeństwa Informacji (ABI)**

**Do zadań Administratora Bezpieczeństwa Informacji należy:**

Stosowanie środków technicznych i organizacyjnych 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:
2. 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;

1. 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.
2. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób.
3. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe.
4. Nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających częstotliwość ich zmiany.
5. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych.
6. Nadzór nad wykonywaniem kopii awaryjnych.
7. Nadzór nad systemem komunikacji w sieci komputerowej.
8. Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
9. Kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane).
10. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń.
11. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe.
12. Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.
13. Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.

Zał. Nr 2

do Zarządzenia Nr 0050.55.2015

Burmistrza Miasta i Gminy Suchedniów

z dnia 30 czerwca 2015r.

**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 oraz ABI, sposobu określania uprawnień w systemach informatycznych.
2. Realizacja decyzji ADO 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.

1. Planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie Miasta i 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. Monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników.

1. Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
2. Nadzorowanie zasad ochrony, przechowywania i niszczenia kopii zapasowych, zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania.
3. Zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych.
4. Zapewnienie awaryjnego zasilania komputerów lub innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
5. Zarządzanie hasłami użytkowników i przestrzeganie procedur określających częstotliwość ich zmiany.

9. Systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego.

10. Zapewnienie eksploatowanym systemom opieki serwisowej producenta – zawieranie umów regulujących formy tej opieki.

11. Rozwiązywanie, samodzielnie i we współpracy z informatykiem, problemów towarzyszących eksploatacji systemów informatycznych.

12. Przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji.

13. Prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT.