ZARZĄDZENIE NR 42/2015
WÓJTA GMINY RZEKUŃ

z dnia 22 czerwca 2015 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Gminy w Rzekuniu.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2013 r. poz. 594 ze zm.), art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r., poz. 1182 ze zm.), zarządzam co następuje:,

§ 1.

1. Wyznaczam **PanaLeszka Zbigniewa Kleczkowskiego** na Administratora Bezpieczeństwa Informacji **(ABI)** w Urzędzie Gminy w Rzekuniu . Zakres działania ABI stanowi załącznik Nr 1 do niniejszego zarządzenia.

2. Wyznaczam **Pana Tomasza Ryszarda Majewskiego** na Administratora Systemów Informatycznych **(ASI)** w Urzędzie Gminy w Rzekuniu. Zakres działania ASI stanowi załącznik Nr 2 do niniejszego zarządzenia.

§ 2.

Traci moc zarządzenie Nr 50/2009 Wójta Gminy Rzekuń z dnia 2 listopada 2009 roku w sprawie wyznaczenia Administratora bezpieczeństwa informacji, Administratora systemu informatycznego służącego oraz osoby upoważnionej do zastępstwa Administratora bezpieczeństwa informacji.

§ 3.

Wykonanie zarządzenie powierzam Sekretarzowi Gminy Rzekuń.

§ 4.

Zarządzenie wchodzi z dniem podpisania.

Wójt Gminy Rzekuń

mgr Stanisław Godzina

Załącznik do Zarządzenia Nr 42/2015

Wójta Gminy Rzekuń

z dnia 22 czerwca 2015 r.

Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

Do zadań Administratora Bezpieczeństwa Informacji należy:

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

1) Zapewnienie 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 aktualizacja dokumentacji, o której mowa w art. 36 ust.2, oraz przestrzegania zasad w niej określonych,
   c) zapewnienie 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 ora Nadzór nad przestrzeganiem procedur określających częstotliwość zmiany haseł.
4) Nadzór nad przestrzeganiem procedur określających częstotliwość zmiany haseł.
5) Nadzór nad czynnościami związanymi ze sprawdzeniem systemu pod kątem obecności wirusów komputerowych.
6) Nadzór nad wykonaniem kopii awaryjnych.
7) Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
8) Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
9) Kontrola nad danymi osobowymi wprowadzanymi do zbiorów (przez kogo zostały wprowadzone, komu zostały przekazane).
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.
14) Prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku przetwarzania danych osobowych.

Załącznik Nr 2 do Zarządzenia Nr 42/2015 Wójta

Gminy Rzekuń z dnia 22 czerwca 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 (innych) odnośnie nadania osobom uprawnień dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania, w środowisku IT Urzędu tj.:
   a) tworzenie kont użytkowników w systemach informatycznych,
   b) przypisywanie, do kont, startowych haseł uwierzytelniających użytkowników tych kont,
   c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
   d) resetowanie utraconych haseł,
   e) usuwanie kont i uprawnień dla kont osób które zakończyły pracę w Urzędzie,
   f) dostarczanie ABI informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych.
3) Planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych.
4) Automatyzacja zadań konserwacyjnych w systemie – w tym wykonywania kopii zapasowych oprogramowania i danych.
5) Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
6) Zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych.
7) Systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego.
8) Przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji.