Zarządzenie Nr 39/2015
Wójta Gminy Stolno
z dnia 15 kwietnia 2015 r.

w sprawie powołania Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Gminy Stolno

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r. poz. 594 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.) oraz w związku z § 37 pkt. 5 Regulaminu Organizacyjnego Urzędu Gminy Stolno, zarządzam, co następuje:

§ 1

1. Wyznaczam Pana Roberta Dobek na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Gminy Stolno. Zakres działania ABI stanowi załącznik Nr 1 do niniejszego zarządzenia.
2. Wyznaczam Pana Janusza Frąckiewicza na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Stolno. Zakres działania ASI stanowi załącznik Nr 2 do niniejszego zarządzenia.

§ 2

Zobowiązuję pracowników Urzędu Gminy Stolno do współpracy z Administratorem Bezpieczeństwa Informacji oraz Administratorem Systemów Informatycznych i wykonywania ich poleceń w zakresie realizacji zadań dotyczących ochrony i bezpieczeństwa przetwarzanych danych w Urzędzie Gminy Stolno

§ 3

Zobowiązuję pracownika na stanowisko ds. obywatelskich i organizacyjnych Urzędu Gminy Stolno do zapoznania wszystkich pracowników Urzędu z treścią niniejszego zarządzenia.

§ 4

Tracą moc: Zarządzenie Nr 36/2011 Wójta Gminy Stolno z dnia 29 kwietnia 2011 r. w sprawie powołania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Stolno oraz Zarządzenie Nr 37/2011 Wójta Gminy Stolno z dnia 29 kwietnia 2011 r. w sprawie powołania Administratora Systemu Informatycznego w Urzędzie Gminy Stolno.

§ 5

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
mgr inż. Jerzy [illegible]

Załącznik Nr 1 do Zarządzenia Nr 39/2015
Wójta Gminy Stolno
z dnia 15 kwietnia 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:
   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. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
5. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisywane są dane osobowe.
6. Nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających częstotliwość ich zmiany.
7. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych.
8. Nadzór nad wykonywaniem kopii awaryjnych.
9. Nadzór nad systemem komunikacji w sieci komputerowej.
10. Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
11. Kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane).
12. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń.
13. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe.
14. Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.
15. Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.
16. Inne zadania określone przepisami prawa, wewnętrznymi aktami wydanymi przez Wójta Gminy Stolno oraz wynikające z polecenia Administratora Danych Osobowych.

Załącznik Nr 2 do Zarządzenia Nr 39/2015
Wójta Gminy Stolno
z dnia 15 kwietnia 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.:
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. Monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników.
7. Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
8. Zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych.
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 pozostałym personelem IT, 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.
14. Inne zadania określone przepisami prawa, wewnętrznymi aktami wydanymi przez Wójta Gminy Stolno oraz wynikające z polecenia Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji.