**Zarządzenie Nr ADM/144/2017  
Wójta Gminy Starogard Gdański**

z dnia 23 listopada 2017 r.

**w sprawie wyznaczenia Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Starogard Gdański.**

Na podstawie art. 33 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym ( Dz. U. z 2017 r., poz. 1875) w związku z Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r., poz. 745) oraz art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922) zarządza się, co następuje:

**§ 1.**Wyznaczam Pana Sebastiana Rogowskiego na Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Starogard Gdański. Zakres Działania ASI stanowi załącznik do niniejszego zarządzenia.

**§ 2.**Odwołuję Pana Włodzimierza Bielińskiego z Administratora Systemów Informatycznych (ASI) w Urzędzie Gminy Starogard Gdański.

**§ 3.**Traci moc § 1 pkt 2 oraz § 3 Zarządzenia Nr ADM/03/2010 Wójta Gminy Starogard Gdański z dnia 5 stycznia 2010 r. w sprawie powołania administratora bezpieczeństwa informacji i administratora systemu informatycznego oraz wdrożenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych

**§ 4.**Zarządzenie wchodzi w życie 1 grudnia 2017 roku.

|  |  |
| --- | --- |
|  |  |

Załącznik do Zarządzenia Nr ADM/144/2017  
Wójta Gminy Starogard Gdański  
z dnia 23 listopada 2017 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 Ujedzie,

f) 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) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,

15) nadzór nad czynnościami związanymi z prowadzeniem systemu w zakresie obecności wisusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywanych procedur uaktualniania systemów antywirusowych i ich konfiguracji,

16) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych,

17) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami sprzętu IT systemów informatycznych aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe,

18) prowadzenie ewidencji sprzętu komputerowego.