

Zarządzenie nr 64/2016
Wójta Gminy Smyków
z dnia 31 sierpnia 2016 r.

w sprawie: wyznaczenia Administratora Systemu Informatycznego w Urzędzie Gminy Smyków oraz określenia jego zakresu działania.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2016 r. poz. 992) zarządzam, co następuje:

§1

Wyznaczam Pana **Mateusza Kuletę**, właściciela firmy Mateusz Kuleta Core-Serwis Miedziera 91, 26-212 Smyków na **Administratora Systemu Informatycznego (ASI)** w Urzędzie Gminy Smyków.

§2

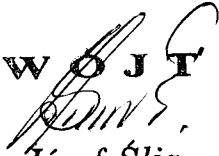
Ustala się zakres działania Administratora Systemu Informatycznego w Urzędzie Gminy Smyków określony w załączniku nr 1 do zarządzenia.

§3

Traci moc zarządzenie nr 165/2012 z dnia 16 listopada 2012 roku w sprawie wyznaczenia Administratora Systemów Informatycznych oraz określenia jego zakresu działania.

§4

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJTA

Józef Śliz

Zakres działania Administratora Sytemu Informatycznego w Urzędzie Gminy Smyków

1. Administrator Systemu Informatycznego, zwany dalej ASI, wykonuje zadania w zakresie „Polityki Bezpieczeństwa Urzędu Gminy Smyków” oraz „Instrukcji Zarządzania Systemem Informatycznym Urzędu Gminy Smyków” oraz upoważnień i pełnomocnictw nadanych przez Administratora Danych Osobowych.
2. Celem działania ASI jest nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w systemach informatycznych Urzędu Gminy Smyków.
3. Zadaniem ASI jest realizacja przedsięwzięć określonych w art. 36 ust. 1 i w art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
4. ASI, realizując swoje zadania współpracuje z Administratorem Bezpieczeństwa Informacji Urzędzie Gminy Smyków.
5. Do zakresu zadań ASI należy w szczególności:
 - 1) monitorowanie:
 - a) zbierania, przechowywania, przekazywania i udostępniania danych osobowych przetwarzanych w systemach informatycznych,
 - b) zabezpieczeń systemów informatycznych w zakresie stosowania:
 - IPS/firewall/VPN oraz programów antywirusowych,
 - szyfrowania dysków i środków ochrony kryptograficznej,
 - mechanizmów autoryzacji i kontroli dostępu do danych (uwierzytelnianie użytkowników, hasła, identyfikatory)
 - zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do baz danych osobowych,
 - 2) nadzorowanie:
 - a) zakładania, blokowania, zawieszania i uaktywniania kont w systemie informatycznym,
 - b) logicznych i informatycznych zabezpieczeń systemów w zakresie:
 - przepływu informacji pomiędzy systemami informatycznymi a siecią publiczną,
 - działań inicjowanych z sieci i z systemów informatycznych

- c) umów i procedur przekazywania podmiotowi zewnętrznemu dostępu do systemów informatycznych oraz elektronicznych nośników informacji zawierających dane osobowe,
 - d) tworzenia kopii zapasowych zbiorów danych osobowych,
 - e) zasad ochrony, przekazywania i niszczenia kopii zapasowych zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania,
- 3) realizowanie przedsięwzięć w zakresie:
- a) wyjaśniania i dokumentowania, wspólnie z ABI, przypadków naruszenia zasad bezpieczeństwa systemów informatycznych,
 - b) prowadzenia opisu struktur zbiorów danych osobowych oraz schematów przepływu danych pomiędzy systemami informatycznymi,
 - c) dokonywania oceny zgodności programów z przepisami bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych,
 - d) kontrolowania, wspólnie z ABI, pracowników w zakresie przestrzegania zasad bezpieczeństwa systemów informatycznych,
 - e) przygotowywanie i nadzorowanie, wspólnie z ABI, wniosków o zgłoszenie zbiorów do rejestru zbiorów danych osobowych ABI lub w Biurze Generalnego Inspektora Ochrony Danych Osobowych oraz aktualizacji tych zgłoszeń.