

Załącznik Nr 1
do Zarządzenia Nr 1061/2017
Burmistrza Pyrzyc
z dnia 12 października 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.:
 - 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. Naprawa, konserwacja oraz likwidacja urządzeń komputerowych, na których zapisane są dane adresowe.
15. Wykonywanie czynności związanych z prowadzeniem systemu w zakresie obecności wirusów komputerowych, częstotliwości ich sprawdzania oraz nadzorowanie wykonywanych procedur, uaktualniania systemów antywirusowych i ich konfiguracji.
16. Konserwowanie oraz aktualizowanie systemów służących do przetwarzania danych osobowych.
17. Wykonywanie przeglądów i konserwacji zgodnie z odrębnymi procedurami sprzętu IT, systemów informatycznych, publikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.
18. Prowadzenie ewidencji sprzętu komputerowego.