

### **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 Inspektorem Ochrony Danych. Do zadań Administratora Systemu Informatycznego należy:

1. Formułowanie, w uzgodnieniu z administratorem danych i/lub osobami, do których administrator delegował zarządzanie uprawnieniami oraz IOD, sposobu określania uprawnień w systemach informatycznych.
2. Realizacja decyzji dotyczących nadawania 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 Starostwie Powiatowym,
  - f) dostarczanie IOD informacji potrzebnych do oceny prawidłowości funkcjonowania sprzętowo-programowych.
3. Planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Starostwie Powiatowym.
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 IOD instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji.

13. Prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemu IT.