

ZADANIA, OBOWIĄZKI, ZAKRES UPRAWNIENÍ I ODPOWIEDZIALNOŚCI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI.

I. Zakres odpowiedzialności.

- 1) Administrator bezpieczeństwa informacji odpowiedzialny jest za zabezpieczenie zbiorów danych znajdujących się w systemie informatycznym przed nieuprawnionym dostępem oraz zniszczeniem.

II. Zakres obowiązków.

- 1) Identyfikacja i analiza zagrożeń związanych z przetwarzaniem i archiwizacją danych osobowych w systemie informatycznym.
- 2) Określenie potrzeb w zakresie zabezpieczeń serwerów baz danych, stanowisk dostępowych, sieci teleinformatycznej oraz sieci energetycznej zasilającej system.
- 3) Nadzór nad prawidłową konfiguracją systemów operacyjnych i systemów bazodanych na serwerach danych osobowych.
- 4) Nadzór nad wdrożeniem polityki bezpieczeństwa w Urzędzie Miejskim w Pabianicach.
- 5) Nadzór nad działaniem urządzeń podtrzymujących zasilanie i właściwą konfigurację oprogramowania monitorującego ich działanie.
- 6) Nadzór nad komputerami przenośnymi, na których znajdują się dane osobowe.
- 7) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych oraz nośników, na których przechowywane są dane osobowe.
- 8) Nadzór nad działaniami firm zewnętrznych w systemie informatycznym.
- 9) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych na pośrednictwem urządzeń teletransmisji.
- 10) Nadzór czynności związanych ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, w tym nadzór na aktualizacją stosownego oprogramowania.
- 11) Nadzór nad przeglądami, konserwacją oraz uaktualnieniami systemów służących do przetwarzania danych osobowych.
- 12) Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.
- 13) Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych.

- 14) Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło i przygotowanie oraz przedstawienie administratorowi danych zmian do instrukcji zarządzania systemem informatycznym służących wyeliminowaniu lub ograniczeniu wystąpień podobnych sytuacji w przyszłości.
- 15) Wnioskowanie do administratora danych o ukaranie osób nie wypełniających postanowień " Instrukcji określającej sposób zarządzania systemem informatycznym w urzędzie Miejskim w Pabianicach " bądź poleceń wymienionych w 3 pkt. 5.
- 16) Zgłaszanie do administratora danych wszelkich zmian w zbiorach danych osobowych.

III. Zakres uprawnień.

Administrator bezpieczeństwa informacji posiada uprawnienia do:

- 1) Wyłączenia elementów systemu informatycznego w sytuacjach zagrażających bezpieczeństwu, bądź integralności zbiorów danych osobowych.
- 2) Wstępu do pomieszczeń w których przetwarzane są dane osobowe.
- 3) Kontroli stanowisk dostępowych oraz informatycznych nośników danych.
- 4) Wydawania wiążących poleceń użytkownikom systemu informatycznego, dotyczących bezpieczeństwa i ochrony danych osobowych oraz środków ich przetwarzania.
- 5) Występowanie do administratora danych w zakresie środków technicznych i organizacyjnych niezbędnych dla poprawnego i bezpiecznego przetwarzania danych osobowych.
- 6) Występowania do administratora danych oraz administratorów bezpieczeństwa ze wszelkimi sprawami dotyczącymi przetwarzania danych osobowych.