ZARZĄDZENIE NR 3/2012
Dyrektora Domu Pomocy Społecznej w Machowinku
z dnia 27.04.2012r.

w sprawie Administratora Bezpieczeństwa Informacji

Na podstawie: Ustawy z dnia 29 sierpnia 1997 roku (Dz.U.Nr 101, poz. 926 z 2002r. ze zm.) o ochronie danych osobowych, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Dyrektor Domu Pomocy Społecznej w Machowinku
zarządza, co następuje:

§ 1

Administratorem Bezpieczeństwa Informacji w Domu Pomocy Społecznej w Machowinku wyznaczony zostaje Referent – Elwira Ruła.

§ 2

Zakres czynności Administratora Bezpieczeństwa Informacji określa załącznik nr 1 do niniejszego Zarządzenia.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

§ 4

Traci moc Zarządzenie wewnętrzne nr 18/2005 z dnia 12.09.2005r. w sprawie Administratora Bezpieczeństwa Informacji.

Załącznik Nr 1 do zarządzenia nr /2012
Dyrektora DPS Machowinko
z dnia 25.04.2012r.

Zakres praw i obowiązków Administratora Bezpieczeństwa Informacji

1. Administrator Bezpieczeństwa Informacji odpowiada za bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych w zakresie zgodności zasad postępowania przy przetwarzaniu danych z obowiązującymi przepisami o ochronie danych osobowych.

2. Do zadań Administratora Bezpieczeństwa Informacji należy w szczególności:

   1) Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzano dane osobowe oraz kontrolą przebywających w nich osób.
   2) Zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
   3) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
   4) Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany.
   5) Nadzór nad czynnościami związanymi z prowadzeniem systemu w zakresie obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywanych procedur uaktualnienia systemów antywirusowych i ich konfiguracji.
   6) Nadzór nad wykonywaniem i przechowywaniem kopii awaryjnych.
   7) Nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych.
   8) Prowadzenie ewidencji wydanych upoważnień i oświadczeń
   9) Szkolenie pracowników z zakresu ochrony danych oraz informowanie użytkowników o zmianach w systemie ochrony danych osobowych