ZARZĄDZENIE Nr.....125...../2015
Burmistrza Głuszycy
z dnia 30 czerwca 2015 roku

w sprawie:**powołania Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Gluszycy**

Na podstawie art. 33 ustawy z dnia 08 marca 1990 roku o samorządzie gminnym (t.j.Dz.U. z 2013 r., poz.594 ze zm.) , art.36a ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r., poz.1182), zarządzam co następuje:

§ 1 Wyznaczam Panią Wiesławę Moździerz na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Miejskim w Głuszycy. Zakres działania ABI stanowi załącznik Nr 1 do niniejszego zarządzenia

§ 2. Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ GŁUSZYCY
Roman Głód

RADCA PRAWNY
mgr Artur Nazimek
WŁ. 332

Załącznik Nr 1

Zakres działania Administratora Bezpieczeństwa Informacji (ABI)

Do zadań Administratora Bezpieczeństwa Informacji należy:

Stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
2. Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
3. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywających w nich osób.
4. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych.
5. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisywane są dane osobowe.
6. Nadzór nad zarządzaniem hasłami użytkowników i przestrzeganiem procedur określających częstotliwość ich zmiany.
7. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych.
8. Nadzór nad wykonywaniem kopii awaryjnych.
9. Nadzór nad systemem komunikacji w sieci komputerowej.
10. Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
11. Kontrola nad danymi osobowymi wprowadzonymi do zbiorów (przez kogo zostały wprowadzone, komu są przekazywane).
12. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń.
13. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe.
14. Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.
15. Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.