Załącznik Nr 1
do Zarządzenia Nr ...159.../2016
Burmistrza Pyrzyc
z dnia..12..grudnia 2016 r.

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.

Administratora Bezpieczeństwa Informacji (ABI) upoważniony jest do:

1. Wydawania poleceń pracownikom Urzędu Miejskiego w Pyrzycach w zakresie związanym ze wdrażaniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.
2. Rozstrzygania sporów dotyczących stosowania i interpretacji wymagań zawartych w dokumentach Systemu Zarządzania Bezpieczeństwem Informacji oraz wydawania wiążących decyzji w tym zakresie.
3. Dostępu do wszystkich dokumentów występujących w Urzędzie Miejskim w Pyrzycach, których treść może być istotna z punktu widzenia funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji.
4. Uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach Systemu Zarzadzania Bezpieczeństwem Informacji.
5. Podejmowania decyzji w kwestiach bezpieczeństwa informacji w zakresie nierodzącym zobowiązań finansowych, w szczególności w zakresie współpracy Urzędu Miejskiego w Pyrzycach z zewnętrznymi jednostkami organizacyjnymi.

KIEROWNIK WYDZIAŁU
Dorota Grzybowska

Załącznik Nr 2
do Zarządzenia Nr ...159.../2016
Burmistrza Pyrzyc
z dnia 13...grudnia 2016 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.

KIEROWNIK WYDZIAŁU
Dorota [illegible]