Zarządzenie Nr 17
Burmistrza Miasta i Gminy Ryn
z dnia 10 lutego 2015r.

w sprawie wyznaczenia administratora bezpieczeństwa informacji oraz upoważnienia do wykonywania zadań lokalnego administratora systemu rejestrów i systemów teleinformatycznych wykorzystywanych w Urzędzie Miasta i Gminy Ryn.

Na podstawie art. 36 ust. 3 i art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. z 2014r. Poz. 1182), 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 (Dz. U. Nr 100, poz. 1024) oraz Regulaminu Organizacyjnego Urzędu Miasta i Gminy Ryn zarządzam, co następuje:

§ 1. wyznaczam Panią Barbarę Kowalską zatrudnioną w Urzędzie Miasta i Gminy Ryn na stanowisku Sekretarza Gminy - na Administratora Bezpieczeństwa Informacji (ABI). Obowiązki ABI określa załącznik Nr 1 do Zarządzenia.

§ 2. upoważniam Pana Tomasza Alończyka do wykonywania zadań Lokalnego Administratora Systemu teleinformatycznego (LAS) wykorzystywanego w Urzędzie, na potrzebę realizacji zadań określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz w Rozporządzeniu Rady Ministrów 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 (Dz. U. Nr 100, poz. 1024)) w odniesieniu do danych osobowych przetwarzanych w zbiorach danych osobowych prowadzonych w Urzędzie Miasta i Gminy Ryn
– na czas nieoznaczony.
Obowiązki LAS określa załącznik Nr 2 do zarządzenia.

§ 3.Traci moc Zarządzenie Nr 19/99 Burmistrza Miasta i Gminy Ryn z dnia 26.10.1999r. w sprawie powołania administratora bezpieczeństwa informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Miasta i Gminy Ryn
Józef Karpiński

Załącznik Nr 1
do Zarządzenia Nr 17
Burmistrza Miasta i Gminy Ryn
z dnia 10.02.2015r.

# Zakres obowiązków
# Administratora Bezpieczeństwa Informacji
# w Urzędzie Miasta i Gminy Ryn

1. Określanie wagi i znaczenia informacji gromadzonych i przetwarzanych
   w Urzędzie w celu realizacji jego zadań;
2. Koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych w Urzędzie, jego poszczególnych działach, sekcjach i samodzielnych stanowiskach;
3. Uwzględnienie prawnych aspektów w procesie zabezpieczenia przetwarzania danych z uwzględnieniem zabezpieczenia systemu informatycznego;
4. Akceptacja lub wyrażanie potrzeby obniżenia poziomu ryzyka związanego
   z przetwarzaniem informacji w Urzędzie;
5. Proponowanie sposobu realizacji mechanizmów ochrony danych z uwzględnieniem specyfiki pracy danej komórki organizacyjnej;
6. Określanie i nadzór nad wdrożeniem, standardów zabezpieczeń informacji
   w Urzędzie;
7. Opiniowanie wszelkich zmian zachodzących przy procesie przetwarzania danych pod kątem ich wpływu na bezpieczeństwo;
8. Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa systemu informatycznego i wyciąganie konsekwencji dyscyplinarnych wobec podległych sobie pracowników zamieszanych w tego typu incydenty;
9. Koordynacja procesu reakcji na incydenty w zakresie naruszenia bezpieczeństwa informacji ;
10. Koordynacja działań związanych z uświadomieniem pracownikom znaczenia ochrony informacji.

Załącznik Nr 2
do Zarządzenia Nr 17
Burmistrza Miasta i Gminy Ryn
z dnia 10.02.2015r.

# Zakres obowiązków
# Lokalnego Administratora Systemu Informatycznego
# w Urzędzie Miasta i Gminy Ryn

1. Implementacja odpowiednich mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej;
2. Merytoryczne przygotowanie i przeprowadzenie szkoleń w zakresie zachowania bezpieczeństwa przy przetwarzaniu danych;
3. Nadawanie uprawnień użytkownikom systemu informatycznego zgodnie z wnioskami ich przełożonych;
4. Zapewnienie podstawowego szkolenia w zakresie korzystania z systemu informatycznego nowo przyjętych pracowników;
5. Odbieranie uprawnień użytkownikom, u których zakończył się okres zatrudnienia;
6. Zapewnienie pomocy użytkownikom przy korzystaniu z systemu informatycznego;
7. Tworzenie kopii zapasowych danych przechowywanych w systemie informatycznym;
8. Zarządzanie licencjami;
9. Monitorowanie poziomu bezpieczeństwa w systemie informatycznym, a w szczególności bieżącego stanu aktualizacji systemów operacyjnych i serwerów oraz sygnatur programów antywirusowych;
10. Monitorowanie działania systemu informatycznego i przekazywanie informacji o zagrożeniach osobie ABI, a w przypadku jego nieobecności bezpośrednio osobie ADO;
11. Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwania ich skutków.
12. Zarządzanie określonymi rozwiązaniami technicznymi związanymi z ochroną systemu informatycznego;
13. Kontrolowanie przestrzegania zasad bezpiecznego przetwarzania danych w

systemie informatycznym;

14. Czasowe przeglądy i weryfikacja m.in.:

    1) ilości i wykazu pomieszczeń dopuszczonych do przetwarzania danych,

    2) rozmieszczenia stacji roboczych w poszczególnych pomieszczeniach,

    3) sprawności użytkowanego sprzętu,

    4) legalności zainstalowanego oprogramowania,

    5) poprawności instalacji łatek systemowych i aktualizacji sygnatur wirusów programu antywirusowego,

    6) przyznanych uprawnień do baz danych;

    7) weryfikacja harmonogramu logowania do systemu informatycznego dla poszczególnych użytkowników.