ZARZĄDZENIE Nr 20/2013

Burmistrza Bornego Sulinowa

z dnia 18 lutego 2013 r.

w sprawie wyznaczenia i określenia zadań Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego w Urzędzie Miejskim w Bornem Sulinowie

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.) w związku z art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) **zarządzam,** co następuje:

§ 1. 1. Wyznaczam Pana Wiesława Fabisińskiego na Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Bornem Sulinowie.

2. Ustalam zakres zadań i uprawnień Administratora Bezpieczeństwa Informacji, stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2. 1. Wyznaczam Pana Kacpra Kobyłeckiego na Administratora Systemu Informatycznego w Urzędzie Miejskim w Bornem Sulinowie.

2. Ustalam zakres zadań Administratora Systemu Informatycznego, stanowiący załącznik nr 2 do niniejszego zarządzenia.

§ 3. Wykonanie zarządzenia powierzam Sekretarzowi Gminy Borne Sulinowo.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
do Zarządzenia nr 20/2013
Burmistrza Bornego Sulinowa
z dnia 18 lutego 2013 r

Zakres zadań i uprawnienia Administratora Bezpieczeństwa Informacji

1. Administrator Bezpieczeństwa Informacji - zwany dalej ABI wykonuje zadania w zakresie niniejszego zarządzenia.

2. Celem działania ABI jest nadzorowanie i kontrolowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w Urzędzie Miejskim. Zadaniem ABI jest realizacja przedsięwzięć określonych art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz 926 z późn. zm.), a w szczególności nadzorowanie i kontrolowanie:

1) stosowania środków technicznych i przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednich do zagrożeń oraz kategorii danych,

2) zabezpieczenia danych osobowych przed udostępnieniem osobom nieupoważnionym zabraniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem,

3) przetwarzania danych osobowych zgodnie z przepisami w/w ustawy.

3. ABI realizując swoje zadania współpracuje z Administratorem Systemu Informatycznego (ASI). Do szczegółowych czynności ABI zaliczyć można:

1) nadzorowanie i kontrolowanie przestrzegania zasad:

a) przetwarzania danych osobowych przez użytkowników zgodnie z zakresem nadanego im upoważnienia,

b) prowadzenia dokumentacji przetwarzania danych osobowych,

c) stosowania przez użytkowników zasad przetwarzania danych osobowych, a w szczególności ich zbierania, utrwalania, opracowywania, zmieniania, udostępniania i ich usuwania,

d) ochrony obszarów przetwarzania danych w zakresie adekwatności stosowanych zabezpieczeń i możliwości wystąpienia w nich zagrożeń,

e) wyposażenia oraz zabezpieczenia pomieszczeń, w których przechowuje się dane sensytywne i kopie zapasowe zbiorów,

f) rejestracji zbiorów w Biurze Generalnego Inspektora Ochrony Danych Osobowych (GIODO) lub zmian przetwarzania danych osobowych.

2) realizowanie zadań w zakresie:

a) rozpatrywania skarg i wniosków dotyczących przetwarzania i ochrony danych,

b) tworzenia projektów zarządzeń, instrukcji i wytycznych Administratora Danych Osobowych,

c) przygotowywania informacji w zakresie rejestracji zbiorów w GIODO lub zmian w przetwarzaniu danych,

d) wyjaśniania i dokumentowania przypadków naruszania zasad przetwarzania i ochrony danych osobowych,

e) organizowania szkoleń z zakresu przetwarzania i ochrony danych osobowych,

f) odnotowywania i dokumentowania zmian w lokalizacjach obszarów przetwarzania danych,

g) wykonywania okresowych analiz zagrożeń bezpieczeństwa i ocen stanu ochrony danych osobowych przetwarzanych w obszarach.

4. Wykonując swoje czynności ABI działa w imieniu Administratora Danych Osobowych i posiada uprawnienia do:

1) wskazywania zastosowania odpowiednich zabezpieczeń technicznych i wykonywania czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych,

2) parafowania umów dotyczących udostępniania lub powierzania danych do przetwarzania osobom lub podmiotom zewnętrznym w zakresie stosowania w nich zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych,

3) wnioskowania o ograniczenie zakresu przetwarzania danych osobowych użytkownikom, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych,

4) udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie kontroli i dostosowania ochrony danych do stanu zgodnego z przepisami prawa,

5) zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących spowodowania zagrożenia bezpieczeństwa danych.

Załącznik nr 2
do Zarządzenia nr 20/2013
Burmistrza Bornego Sulinowa
z dnia 18 lutego 2013 r

Zakres zadań Administratora Systemu Informatycznego.

Administrator Systemu Informatycznego - zwany dalej ASI, wykonuje zadania w zakresie niniejszego zarządzenia, a w szczególności:

1) nadawanie identyfikatorów użytkownikom danych osobowych,

2) zabezpieczenie i kontrolowanie prawidłowości przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,

3) pozbawianie zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie urządzeń lub nośników, które przeznaczone są do likwidacji,

4) instalowanie zabezpieczeń w systemach informatycznych,

5) wyrejestrowywanie i rejestrowanie z systemu użytkowników w czasie instalowania oraz modyfikacji systemu,

6) przydzielanie uprawnień do poszczególnych systemów,

7) wykonywanie kopii awaryjnych danych z serwera, właściwe przechowywanie nośników, sprawdzanie poprawności zapisu oraz ich likwidowanie,

8) dokonywanie wyboru lub migracji do technologii minimalizującej zagrożenia uzyskania dostępu do sieci osobom nieupoważnionym,

9) nadzorowanie procesu monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych,

10)wykonywanie poleceń Administratora Bezpieczeństwa Informacji w zakresie zarządzania podległymi systemami informatycznymi,

11) czuwanie nad właściwym eksploatowaniem podległych mu systemów informatycznych,

12) stwarzanie właściwych warunków organizacyjno-technicznych gwarantujących bezpieczeństwo podległych mu systemów informatycznych,

13) nadzorowanie właściwej lokalizacji sprzętu komputerowego, tj. ustawiania monitorów i drukarek uniemożliwiającego wgląd w dane osobowe osobom nieupoważnionym lub kradzież wymiennych nośników danych,

14)występowanie do Administratora Danych Osobowych z wnioskiem o upoważnienie pracowników do przetwarzania danych osobowych,

15) nadawanie haseł dostępu użytkownikom oraz ustawianie uprawnień w podległych im systemach

16) pozbawianie zapisu danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych,

17) prowadzenie, uaktualnianie na bieżąco oraz przesyłanie Administratorowi Bezpieczeństwa Informacji danych dotyczących:

a) listy użytkowników danych osobowych wraz z przydzielonymi im uprawnieniami do poszczególnych funkcji systemu,

b) lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku jakichkolwiek zmian tych danych,

c) rodzaju systemów informatycznych funkcjonujących w zakresie ich działania,

d) czynności serwisowych wykonywanych w podległych systemach informatycznych,

e) zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytych wirusów, koni trojańskich itp. oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania,

18) zgłaszanie Administratorowi Bezpieczeństwa Informacji potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych.