Burmistrz
Miasta i Gminy
Chmielnik

ZARZĄDZENIE Nr 166/2011
BURMISTRZA MIASTA I GMINY CHMIELNIK
z dnia 28 grudnia 2011 roku

w sprawie: zmiany Administratora Bezpieczeństwa Informacji oraz powołania Administratora Systemu Informatycznego służącego do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Chmielniku.

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jednolity Dz. U. z 2001 r. Nr 142 poz. 1591 ze zmianami) oraz art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst Dz. U. z 2002 r. Nr 101 poz. 926 z późniejszymi zmianami) zarządzam co następuje:

§1.

Odwołuję z funkcji Administratora Bezpieczeństwa Informacji w systemie informatycznym w Urzędzie Miasta i Gminy w Chmielniku Pana Adama Stachowicza.

§2.

1. Powołuję na Administratora Bezpieczeństwa Informacji (ABI) w Urzędzie Miasta i Gminy w Chmielniku Pana Damiana Tomaszewskiego.
2. Zakres czynności dla Administratora Bezpieczeństwa Informacji stanowi załącznik nr 1 do niniejszego zarządzenia.

§3.

1. Powołuję na Administratora Systemu Informatycznego (ASI) w Urzędzie Miasta i Gminy w Chmielniku Pana Damiana Tomaszewskiego.
2. Zakres czynności dla Administratora Systemu Informatycznego stanowi załącznik nr 2 do niniejszego zarządzenia.

§4.

Zarządzenie wchodzi w życie z dniem wydania.

Burmistrz
Jarosław Zatorski

Załącznik nr 1
do Zarządzenia Nr 166/2011
Burmistrza Miasta i Gminy w Chmielniku
z dnia 28 grudnia 2011 roku

Zakres czynności Administratora Bezpieczeństwa Informacji (ABI)

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za:

1. Realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji.
2. Ewidencjonowanie lokalnych zbiorów danych osobowych wykorzystywanych w Urzędzie.
3. Zapewnienie dostępu do informacji chronionych wyłącznie przez osoby upoważnione, i wykonujące wyłącznie uprawnione operacje oraz określenie, które osoby i na jakich prawach mają dostęp do danych informacji.
4. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń zabezpieczeń lub podejrzenia naruszenia w systemie.
5. Określenie budynków, pomieszczeń, lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane.
6. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe.
7. Zabezpieczenie obszarów przetwarzania danych osobowych w sposób uniemożliwiający dostęp do nich osób trzecich.
8. Zgłoszenie konieczności uzupełnienia zakresu czynności osoby zatrudnionej przy przetwarzaniu danych o zakres odpowiedzialności tej osoby za ochronę danych do Administratora Informacji.
9. Ewidencjonowanie udostępnionych danych zgodnie z ustawą o ochronie danych osobowych.
10. Weryfikację dopuszczenia użytkowników do przetwarzania danych,
11. Prowadzenie rejestru osób dopuszczonych do przetwarzania danych osobowych i informacji chronionych.
12. Szkolenia osób dopuszczonych do danej grupy informacji chronionych w tym zaznajomienie i przeszkolenie pracowników zatrudnionych przy przetwarzaniu danych osobowych z przepisami ustawy o ochronie danych osobowych i przepisami zawartymi w Polityce bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Chmielniku.
13. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzeniem pod kątem ich dalszej przydatności.
14. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
15. Nadzór nad zgłoszeniem zbioru danych do rejestracji.

Burmistrz
Jarosław Zatorski

Załącznik nr 2
do Zarządzenia Nr 166/2011
Burmistrza Miasta i Gminy w Chmielniku
z dnia 28 grudnia 2011 roku

Zakres czynności Administratora Systemu Informatycznego (ASI)

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. Określenie miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia informacji należącej do danej grupy.
2. Bieżący monitoring oraz zapewnienie ciągłości Działania systemu informatycznego.
3. Optymalizację wydajności systemu informatycznego.
4. Instalację i konfigurację sprzętu sieciowego i serwerowego.
5. Instalację i konfigurację oprogramowania systemowego i sieciowego.
6. Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem.
7. Współpracę z dostawcami usług, sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych.
8. Weryfikację możliwości integracji systemów informatycznych.
9. Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego.
10. Zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie.
11. Opracowanie procedur określających zarządzanie systemem informatycznym.
12. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.
13. Prowadzenie zakupów urządzeń sieciowych i serwerowych.
14. Prowadzenie zakupów oprogramowania sieciowego i serwerowego.
15. Świadczenie pomocy technicznej użytkownikom.
16. Zarządzanie, sprawowanie nadzoru oraz serwis urządzeń komputerowych pracujących w systemie informatycznym.
17. Diagnozowanie zdarzeń i usuwaniu awarii urządzeń komputerowych.
18. Konfigurację i administrację oprogramowaniem systemowym na stacjach roboczych zabezpieczającym dane chronione przed nieupoważnionym dostępem.
19. Archiwizowanie na prośbę użytkownika danych z lokalnych stacji roboczych.
20. Nadzór nad eksploatacją materiałów do drukarek.
21. Prowadzenie ewidencji sprzętu i oprogramowania.
22. Instalację nowo kupionych urządzeń komputerowych, na podstawie zapotrzebowań otrzymanych od poszczególnych pracowników urzędu.
23. Tworzenie kopii awaryjnych danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie z Lokalnych systemów.
24. Koordynację działań zapewniających sprawne funkcjonowanie i zabezpieczenie systemu informatycznego przed niepowołanym dostępem.

25. Analizę raportów wszelkich zdarzeń związanych z bezpieczeństwem systemów przetwarzania informacji chronionych.
26. Zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione i że mogą one wykonywać wyłącznie uprawnione operację.
27. Kontrolę procesu przyznawania praw dostępu.
28. Przygotowanie dokumentów polityki bezpieczeństwa danego systemu przetwarzania informacji chronionych.
29. Przygotowanie dokumentów procedur zarządzania kontami użytkowników.
30. Przygotowanie dokumentów procedur kryzysowych związanych z incydentami.

Burmistrz
Jarosław Zatorski