ZARZĄDZENIE NR 8.2015
STAROSTY OPATOWSKIEGO

z dnia 10 kwietnia 2015 r.

w sprawie powołania administratora bezpieczeństwa informacji i administratora systemów informatycznych Starostwa Powiatowego w Opatowie

Na podstawie 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2013 r. poz. 595, z późn. zm.) oraz art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.), zarządza się, co następuje:

§ 1. 1. Powołuje się z dniem 10 kwietnia 2015 r. panią Joannę Podsiadło do pełnienia zadań Administratora Bezpieczeństwa Informacji Starostwa Powiatowego w Opatowie, z wyłączeniem Powiatowego Zespołu ds. Orzekania o Niepełnosprawności przy pomocy pana Karola Adamskiego Administratora Systemu Informatycznego Starostwa Powiatowego w Opatowie.

2. Wyłączenie, o którym mowa w ust. 1 wynika z art. 6d ust. 2 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnieniu osób niepełnosprawnych (Dz. U. z 2011 r. Nr 127, poz. 721, z późn. zm.).

3. Zadania ABI, zostały określone w załączniku nr 1 do niniejszego zarządzenia.

4. Zadania ASI, zostały określone w załączniku nr 2 do niniejszego zarządzenia.

§ 2. Tracą moc zarządzenia Nr 28/09 i Nr 30/09 z dnia 1 października 2009 r.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA OPATOWSKI

Starosta Opatowski

Bogusław Włodarczyk

Załączniki do zarządzenia Nr 8.2015
Starosty Opatowskiego
z dnia 10 kwietnia 2015 r.

Załącznik nr 1

Obowiązki i Uprawnienia
Administratora Systemu Informatycznego

1. Nadzór nad fizycznym zabezpieczeniem pomieszczenia, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób. Pomieszczenia, o których mowa wyżej powinny być zabezpieczone przed dostępem do nich osób nieposiadających uprawnienia do przetwarzania danych osobowych. Osoby nieposiadające takich uprawnienia mogą przebywać w nich jedynie w obecności osób uprawnionych. Na czas nieobecności zatrudnionych tam osób, pomieszczenia te powinny być odpowiednio zabezpieczone. W celu zabezpieczenia pomieszczenia należy zastosować odpowiednie zamki do drzwi oraz sprawować właściwy nadzór nad kluczami do tych pomieszczenia.

2. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. Komputery oraz urządzenia, o których mowa wyżej powinny być zasilane poprzez zastosowanie specjalnych urządzeń podtrzymujących zasilanie. Urządzenia te powinny być wyposażone w oprogramowanie umożliwiające bezpieczne wyłączenie systemu komputerowego. Oznacza to takie wyłączenie, w którym przed zanikiem zasilania zostaną prawidłowo zakończone rozpoczęte transakcje na bazie danych oraz wszelkie inne działania w ramach pracujących aplikacji i oprogramowania systemowego.

3. Dopilnowanie, aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby mikrokomputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych. Osoby posiadające mikrokomputery przenośne z zapisanymi w nich danymi osobowymi należy przeszkolili w kierunku zachowania szczególnej uwagi podczas ich transportu oraz uczulić na to, aby mikrokomputery te przechowywane były we właściwie zabezpieczonym pomieszczeniu.

4. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych ich konfiguracji.

5. Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.

6. Nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny. W zakresie nadzoru, o którym mowa wyżej administrator bezpieczeństwa informacji powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub już niepotrzebnych wydruków komputerowych z danymi osobowymi.

7. Dopilnowanie, aby w pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych były ustawione w taki sposób, aby uniemożliwid tym osobom wgląd w dane.

8. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie administratorowi danych odpowiednich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych (§11 ust. 1 rozporządzenia). Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości. Obowiązek śledzenia skuteczności za bezpieczeństwo, o którym mowa wyżej oraz obowiązek ich udoskonalania, nałożony na administratora. Bezpieczeństwo, wynika bezpośrednio z obowiązku podejmowania odpowiednich działań w przypadku wykrycia naruszeń w systemie bezpieczeństwa (§ 3 rozporządzenia).

Załącznik nr 2

Obowiązki i Uprawnienia Administratora Systemu Informatycznego

1. Realizacja procedur zawartych w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. Zapewnia awaryjne zasilanie komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.

3. Stosowanie odpowiednich metod i środków uwierzytelnienia informatycznego oraz realizacja procedur związanych z ich zarządzaniem i użytkowaniem.

4. Nadzór nad realizacją przeznaczonych dla użytkowników procedur rozpoczęcia, zawieszenia i zakończenia pracy.

5. Realizacja procedur tworzenia kopii zapasowych zbiorów danych w systemie informatycznym oraz programów i narzędzi programowych służących do ich przetwarzania.

6. Nadzór nad przechowywaniem elektronicznych nośników informatycznych zawierających dane osobowe.

7. Realizacja ochrony przed działaniem osób oraz oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

8. Dopilnowanie właściwego stosowania zasad i sposobów odnotowywania w systemie informatycznym o udostępnianiu danych osobowych.

9. Pozbawianie zapisu danych osobowych na nośnikach informatycznych przeznaczonych do likwidacji w sposób uniemożliwiający odczytanie tych nośników.

10. Realizacja przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

11. Współpraca z Administratorem Bezpieczeństwa Informacji w zakresie ochrony danych osobowych.

12. Nadawanie identyfikatorów i uwierzytelniania w systemie informatycznym.

13. Wnioskowanie do Administratora Danych o wydawanie poleceń służbowych użytkownikom sieci informatycznej i ich przełożonym odnośnie przetwarzania danych osobowych w systemie informatycznym.

14. Kontrola przestrzegania procedur przez użytkowników systemu informatycznego.

15. Wnioskowanie w sprawie bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

16. Prowadzenie szkoleń dotyczących przetwarzania danych w systemie informatycznym.