ZARZĄDZENIE NR 18/2008
STAROSTY PIŃCZOWSKIEGO
z dnia 26 listopada 2008 roku

w sprawie powołania Administratora Bezpieczeństwa Informacji Starostwa Powiatowego w Pińczowie

Działając na podstawie art. 34 ust. 1 i art. 35 ust. 2 Ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (tekst jednolity: Dz. U. z 2001r. Nr 142, poz. 1592 z późn. zm.) art. 4 ust. 4 ustawy z dnia 22 marca 1990r. o pracownikach samorządowych (tekst jednolity: Dz. U. z 2001r. Nr 142, poz. 1593 z późn. zmianami) art. 36 ust. 3 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) zarządza się, co następuje:

§ 1

Wyznacza się z dniem 1 grudnia 2008 roku Pana Michała Klamińskiego do pełnienia obowiązków Administratora Bezpieczeństwa Informacji Starostwa Powiatowego w Pińczowie.

§ 2

Szczegółowy zakres obowiązków Administratora Bezpieczeństwa Informacji określa załącznik nr 1 do niniejszego Zarządzenia.

§ 3

Zobowiązuje się Kierownika Wydziału Organizacyjnego i Spraw Obywatelskich do zapoznania wszystkich pracowników Starostwa z treścią niniejszego Zarządzenia.

§ 4

Wykonanie Zarządzenia powierza się Kierownikowi Wydziału Organizacyjnego i Spraw Obywatelskich Starostwa.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA

dr inż. Andrzej Kozera

Załącznik nr 1
do Zarządzenia Nr 18/2008
Starosty Pińczowskiego

Zakres obowiązków
Administratora Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji jest osobą odpowiedzialną za bezpieczeństwo danych w systemie informatycznym, w tym szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

Wymieniony wyżej zakres odpowiedzialności administratora bezpieczeństwa informacji sprawia, że do jego głównych obowiązków należą:

1. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane oraz kontrola przebywających w nich osób. Pomieszczenia, o których mowa wyżej powinny być zabezpieczone przed dostępem do nich osób nie posiadających uprawnień do przetwarzania danych. Osoby nie posiadające takich uprawnień mogą przebywać w nich jedynie w obecności osób uprawnionych. Na czas nieobecności zatrudnionych tam osób, pomieszczenia te powinny być odpowiednio zabezpieczone.

2. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. komputery oraz urządzenia, o których mowa wyżej powinny być zabezpieczone 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 operacje na bazie danych oraz wszelkie inne działanie w ramach pracujących aplikacji i oprogramowania systemowego.

3. Dopilnowanie, aby komputery przenośne, w których przetwarzane są dane zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby komputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych. Osoby posiadające komputery przenośne lub inne urządzenia jak palmtopy lub tzw. dyski wymienione z zapisanymi w nich danymi należy przeszkolić w celu zachowania szczególnej uwagi podczas ich transportu oraz na to, aby urządzenia te przechowywane były w sposób zabezpieczający dane osobowe.

4. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe. Dyski i inne informatyczne nośniki danych, a w przypadku gdy nie jest to możliwe należy uszkodzić w sposób uniemożliwiający ich odczyt.
urządzenia przekazywane do naprawy należy pozbawić zapisu danych lub naprawiać w obecności osoby upoważnionej przez administratora danych.

5. Zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi, które powinny być zawarte w instrukcji

określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych za szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

6. Nadzór nad wykonywaniem czynności sprawdzających obecność wirusów komputerowych, częstość ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.

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

8. Nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych.

9. Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

10. Nadzór nad obiegiem oraz przechowywaniem dokumentów i informacji generowanych przez system informatyczny. W zakresie nadzoru, o którym mowa wyżej administrator bezpieczeństwa informacji powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub niepotrzebnie już wydruków komputerowych z danymi.

11. Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych.
Nadzorowanie, o którym mowa wyżej powinno obejmować:

- ustalenie identyfikatorów użytkowników i ich haseł (identyfikatory użytkowników należy wpisać do ewidencji osób zatrudnionych przy przetwarzaniu danych).
- dopilnowanie, aby hasła użytkowników były zmieniane, co najmniej raz na miesiąc,
- dopilnowanie, aby dostęp do danych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,
- dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy (również po upływie terminu ich ważności),
- dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zostały natychmiast wyrejestrowane, a ich hasła unieważnione.

12. Dopilnowanie, aby ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane, automatycznie się wyłączały po upływie ustalonego czasu nieaktywności użytkownika. Zalecanym rozwiązaniem powyższego problemu jest zastosowanie takich wygaszaczy ekranowych, które po upływie określonego czasu bezczynności użytkownika wygaszają monitor i jednocześnie uruchamiają blokadę, która uniemożliwia kontynuowanie pracy na komputerze bez podania właściwego hasła. Wygaszacz taki oprócz ochrony danych, które przez dłuższy okres czasu wyświetlane byłyby na ekranie monitora, chroni system przed przechwyceniem sesji dostępu do danych przez nieuprawnioną osobę.

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

14. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa wyżej powinny mieć na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie. Szczegółowe zasady postępowania w przypadku naruszenia zabezpieczeń powinny być określone w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. W przypadku, gdy istnieje podejrzenie, iż naruszenie bezpieczeństwa danych osobowych spowodowane zostało zaniedbaniem lub naruszeniem dyscypliny pracy, zadaniem administratora bezpieczeństwa informacji powinno być przedstawienie wniosku Staroście o wszczęcie postępowania wyjaśniającego i ukaranie odpowiedzialnych za to osób.

15. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych i przygotowanie oraz przedstawienie Staroście odpowiednich zmian do instrukcji zarządzania systemem informatycznym. Zmiany te powinny być takie, aby wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości. Obowiązek udoskonalania, nałożony na administratora bezpieczeństwa, wynika bezpośrednio z obowiązku podejmowania odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

16. Prowadzenie szkoleń użytkowników z zakresu bezpieczeństwa systemu komputerowego lub występowanie z wnioskiem o przeprowadzenie szkoleń użytkowników z zakresu bezpieczeństwa systemu komputerowego.

17. Wykonywanie archiwizacji danych systemu komputerowego, zgodnie z obowiązującymi procedurami.

Podsumowanie:

Wymienione wyżej zadania administratora bezpieczeństwa informacji wskazują jedynie w sposób ogólny zagadnienia dotyczące bezpieczeństwa danych w systemach, gdzie są przetwarzane dane. Niezależnie od wymienionych tam czynności, zadaniem Administratora Bezpieczeństwa Informacji jest śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych w ogóle i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo to wzmocnią. Ponadto Administrator Bezpieczeństwa Informatycznego odpowiedzialny jest za opracowanie i wdrożenie polityki bezpieczeństwa (instrukcje, regulaminy, procedury i dokumentacje).Administrator Bezpieczeństwa Informacji, swoje działania powinien dostosować do sytuacji organizacyjnej oraz finansowej Starostwa. Chodzi tutaj głównie o dobór środków wpływających na bezpieczeństwo danych osobowych w systemie informatycznym oraz na przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane. W przypadku, gdy administrator danych nie jest w stanie zakupić drogich, profesjonalnych informatycznych narzędzi zabezpieczających dane, administrator bezpieczeństwa informacji powinien wskazać tańsze często fizyczne środki zabezpieczające przetwarzane dane, które przy zachowaniu odpowiedniej organizacji pracy mogą być również wystarczające.

STAROSTA

dr inż. Andrzej Kozero