ZARZĄDZENIE NR 253/2008
PREZYDENTA MIASTA KRAKOWA
Z DNIA 7 lutego 2008 roku

w sprawie zmiany zarządzenia Nr 1536/2007 Prezydenta Miasta Krakowa z dnia 18 lipca 2007 roku w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym Urzędu Miasta Krakowa.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142 poz. 1591, z późn. zm.), art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.) oraz 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. z 2004 r. Nr 100 poz. 1024) zarządza się, co następuje:

§ 1

W zarządzeniu Nr 1536/2007 Prezydenta Miasta Krakowa z dnia 18 lipca 2007 roku w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym Urzędu Miasta Krakowa wprowadza się następujące zmiany:

1. § 4 pkt 19 załącznika otrzymuje brzmienie:

„19. *Administratorze Bezpieczeństwa Informacji* – rozumie się przez to osobę odpowiedzialną za nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych w UMK.”.

2. § 5 pkt 9 załącznika otrzymuje brzmienie:

„9. Administratora Bezpieczeństwa Informacji powołuje Dyrektor Magistratu. Zakres odpowiedzialności i kompetencji Administratora Bezpieczeństwa Informacji został określony w Polityce Bezpieczeństwa Informacji Urzędu Miasta Krakowa, przyjętej odrębnym zarządzeniem Prezydenta Miasta Krakowa.”.

3. § 2 pkt 18 załącznika Nr 2 do Instrukcji Zarządzania SI UMK otrzymuje brzmienie:

„18. Co najmniej raz do roku, a w przypadku aplikacji przetwarzających informacje chronione – co sześć miesięcy, Administrator Techniczny jest zobowiązany do przeprowadzenia weryfikacji kont w aplikacji lub oprogramowaniu systemowym, za które jest odpowiedzialny. Administrator Systemu jest zobowiązany do przygotowania odpowiedniej procedury, zgodnie, z którą będzie prowadzona ta weryfikacja.”.

4. § 3 pkt 5 załącznika Nr 2 do Instrukcji Zarządzania SI UMK otrzymuje brzmienie:

„5. W przypadkach stwierdzenia naruszenia Bezpieczeństwa Informacji Chronionych lub Bezpieczeństwa SI UMK, należy niezwłocznie powiadomić o tym bezpośredniego Przełożonego oraz Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną.”.

5. § 3 pkt 10 załącznika Nr 2 do Instrukcji Zarządzania SI UMK otrzymuje brzmienie:

„10. Zabrania się użytkownikowi SI UMK:
1) Podejmować prób wykorzystania obcych identyfikatorów użytkownika (kont) i uruchamiania aplikacji deszyfrujących (łamiących) hasła chyba, że użytkownik jest Administratorem Systemu, Administratorem Technicznym lub Administratorem Bezpieczeństwa Informacji i prowadzi te działania w celu zapewnienia ochrony informacji (np. testowanie zabezpieczeń) przetwarzanych w SI UMK.
2) Prowadzenia działań mających na celu nieautoryzowany dostęp do Informacji Chronionych przetwarzanych w SI UMK lub podsłuchiwanie czy przechwytywanie informacji przepływających w sieci komputerowej, chyba, że użytkownik jest Administratorem Systemu, Administratorem Technicznym lub Administratorem Bezpieczeństwa Informacji i prowadzi te działania w celu zapewnienia ochrony informacji (np. testowanie zabezpieczeń) przetwarzanych w SI UMK.
3) Udostępniać osobom trzecim informacji na temat struktury technicznej SI UMK (w tym adresacji sieci, struktur aplikacji, baz danych itp.) bez zgody Administratora Informacji przetwarzanych w SI, chyba, że użytkownik jest Administratorem Systemu, Administratorem Technicznym lub Administratorem Bezpieczeństwa Informacji.
4) Samodzielnej instalacji oprogramowania systemowego i aplikacji chyba, że użytkownik jest Administratorem Systemu lub Administratorem Technicznym.
5) Uruchamiania aplikacji i programów, które mogą zakłócić i destabilizować pracę SI UMK, bądź naruszyć bezpieczeństwo danych w nim przetwarzanych.
6) Wysyłania niechcianej przez odbiorcę poczty elektronicznej – tzw. *spamu* oraz wysyłania poczty elektronicznej do losowych odbiorców.”.

6. § 5 pkt 1 załącznika Nr 2 do Instrukcji Zarządzania SI UMK otrzymuje brzmienie:

„1. Administrator Informacji przetwarzanych w SI przygotuje Politykę Bezpieczeństwa SI UMK, w której określi co najmniej:
a) szczegółowe zasady dostępu do informacji chronionych, przetwarzanych w SI UMK,
b) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są informacje chronione w SI UMK,
c) szczegółowy podział SI UMK na odpowiednie obszary zróżnicowane pod względem bezpieczeństwa: Intranet, Extranet, DMZ itp.,
d) wykaz zbiorów danych zawierających informacje chronione w SI UMK wraz ze wskazaniem aplikacji zastosowanych do przetwarzania tych danych,
e) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
f) sposób przepływu danych pomiędzy poszczególnymi aplikacjami w SI UMK lub poza System,
g) wymagania dla aplikacji przetwarzających informacje chronione oraz pozostałych aplikacji wchodzących w skład SI UMK,
h) opis postępowania w przypadku wystąpienia sytuacji kryzysowych,

i) sposób postępowania z wydrukami i nośnikami danych zawierającymi informacje chronione przetwarzane w SI UMK.”.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Krakowa
/ - /