ZARZĄDZENIE NR 838/2009
PREZYDENTA MIASTA KRAKOWA
Z DNIA 21 kwietnia 2009 r.

w sprawie wprowadzenia do stosowania oraz określenia zasad korzystania ze Zintegrowanego Systemu Zarządzania Oświatą w Gminie Miejskiej Kraków.

Na podstawie art. 31 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2001 r. Nr 142 poz. 1591, z późn. zm.), art. 34 ust 1 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142 poz. 1592, z późn. zm.) oraz art. 34a ust. 1, 2 ustawy z dnia 7 września 1991 roku o systemie oświaty (tekst jednolity: Dz. U. z 2004 r. Nr 256 poz. 2572, z późn. zm.), art. 36 w związku z art. 3 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.), §6 ust. 4 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. Nr 100 poz. 1024) zarządza się, co następuje:

§1

1. Ilekroć w niniejszym zarządzeniu jest mowa o:
   1) **„Systemie”** – należy przez to rozumieć Zintegrowany System Zarządzania Oświatą w Krakowie;
   2) „**Modułach**” – należy przez to rozumieć części Systemu realizujące określoną funkcjonalność;
   3) **„Dostępie do Systemu”** – należy przez to rozumieć posiadanie konfiguracji tj. indywidualnego loginu i hasła oraz certyfikatu w Systemie;
   4) **„Wydziale”** – należy przez to rozumieć Wydział Edukacji Urzędu Miasta Krakowa;
   5) **„Referacie ds. ZSZO”** – należy przez to rozumieć komórkę organizacyjną Wydziału Edukacji ds. Zintegrowanego Systemu Zarządzania Oświatą;
   6) **„ZEO”** – należy przez to rozumieć Zespół Ekonomiki Oświaty (Kraków – Zachód, Kraków – Wschód i Kraków – Południe) będący miejską jednostką organizacyjną w Krakowie;

7) „**Placówce**” – należy przez to rozumieć przedszkola, szkoły oraz placówki, o których mowa w art. 2 ustawy o systemie oświaty prowadzone przez Gminę Miejską Kraków;
8) **„Użytkowniku”** – należy przez to rozumieć osobę uprawnioną, która uzyskała dostęp do Systemu, przetwarza w nim dane oraz może uzyskać dostęp do informacji chronionych przetwarzanych w Systemie;
9) **„Gospodarzu”** – rozumie się przez to kierującego Wydziałem, ZEO, Placówką osobę właściwą dla danego zakresu danych, odpowiedzialną za merytoryczny nadzór nad pracą aplikacji;
10) „**Koordynatorze**” – rozumie się przez to osobę kierującą Wydziałem, odpowiedzialną za merytoryczny nadzór nad funkcjonowaniem Systemu we wszystkich jego obszarach oraz pracą wszystkich Gospodarzy i Użytkowników;
11) **„Merytorycznym Administratorze Informacji”** – należy przez to rozumieć osobę odpowiedzialną merytorycznie za przetwarzanie zbiorów danych osobowych w Systemie oraz w dyspozycji której znajdują się te zbiory;
12) **„Administratorze Bezpieczeństwa Informacji”** – należy przez to rozumieć osobę odpowiedzialną za nadzór nad bezpieczeństwem zbiorów danych osobowych przetwarzanych w Systemie;
13) **„Administratorze Systemu ”** – należy przez to rozumieć podmiot zajmujący się administrowaniem Systemem, jest on odpowiedzialny za ciągłość pracy, rozwój oraz bezpieczeństwo Systemu, w tym za techniczne przetwarzanie informacji w Systemie oraz za bezpieczeństwo tych informacji;
14) **„Identyfikatorze**” Użytkownika – należy przez to rozumieć ciąg znaków literowych, cyfrowych jednoznacznie identyfikujący osobę, która jest użytkownikiem ZSZO;
15) „**Haśl**e” – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych wykorzystywany w procesie uwierzytelniania Użytkownika przy uzyskiwaniu dostępu do ZSZO i znany jedynie Użytkownikowi;
16) „**Uwierzytelnianiu**” – należy przez to rozumieć proces identyfikacji Użytkownika, czyli ustalenie jego tożsamości na podstawie podanego identyfikatora Użytkownika oraz hasła;
17) „**Autoryzacji**” – należy przez to rozumieć proces weryfikujący, czy dany Użytkownik (o ustalonej w procesie uwierzytelniania tożsamości) ma prawo dostępu do informacji (danych), do których usiłuje uzyskać dostęp;
18) **„Informacjach (danych)”** – należy przez to rozumieć reprezentacje informacji (danych), czyli wszelkie zapisy w układach elektronicznych przetwarzane w Systemie;
19) „**Przetwarzaniu informacji**” – należy przez to rozumieć jakiekolwiek operacje wykonywane na informacji, w szczególności zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, wykonywane w Systemie;

Wprowadzenie Systemu do stosowania

§2

1. Wprowadza się obowiązek zamieszczania informacji w Systemie będącym narzędziem informatycznym wspomagającym pracę:
   1) Placówek;
   2) ZEO;
   3) Wydziału.
2. Dyrektor Wydziału ustala harmonogram uruchamiania poszczególnych modułów, który jest na bieżąco weryfikowany.
3. Zamieszczanie informacji w Systemie przez Placówki i ZEO następuje niezwłocznie po wydaniu polecenia przez Dyrektora Wydziału.
4. Zamieszczanie informacji w Systemie następuje zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.).

Definicja uprawnień i zależności

§3

1. Kierujący Wydziałem pełni funkcje:
   1) Koordynatora Systemu;
   2) Gospodarza Systemu dla zakresu danych Wydziału;
   3) Merytorycznego Administratora Informacji dla zbiorów danych osobowych przetwarzanych przez Wydział.

2. Kierujący ZEO pełni funkcje:
   1) Gospodarza Systemu dla zakresu danych ZEO;
   2) Merytorycznego Administratora Informacji dla zbiorów osobowych przetwarzanych przez ZEO;
   3) Administratora Bezpieczeństwa Informacji dla zbiorów danych osobowych przetwarzanych przez ZEO.

3. Kierujący Placówką pełni funkcje:
   1) Gospodarza Systemu dla zakresu danych Placówki;
   2) Merytorycznego Administratora Informacji dla zbiorów osobowych Placówki;
   3) Administratora Bezpieczeństwa Informacji dla zbiorów danych osobowych Placówki.

4. W przypadku nieobecności kierujących Wydziałem, ZEO i Placówką funkcje powyższe pełnią odpowiednio osoby ich zastępujące.

5. Kierujący ZEO lub Placówką może upoważnić do pełnienia roli Administratora Bezpieczeństwa Informacji inną osobę (wzór upoważnienia stanowi załącznik nr 1 do niniejszego zarządzenia).

6. Użytkownik skonfigurowany w Systemie ma dostęp do danych w nim zawartych zgodnie z indywidualnymi uprawnieniami, w szczególności:
   1) Użytkownik w placówce ma dostęp do danych dotyczących wyłącznie danej placówki, a w przypadku dostępu do danych osobowych stosownie do wydanego przez Merytorycznego Administratora Informacji upoważnienia do przetwarzania danych osobowych (wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszego zarządzenia);
   2) Użytkownik w ZEO ma dostęp do danych dotyczących danego ZEO oraz może posiadać dostęp do danych dotyczących wyznaczonych placówek obsługiwanych przez ZEO, a w przypadku dostępu do danych osobowych stosownie do wydanych przez Merytorycznych Administratorów Informacji upoważnień do przetwarzania danych osobowych;
   3) Użytkownik w Wydziale ma dostęp do danych dotyczących Wydziału oraz może posiadać dostęp do danych dotyczących ZEO i placówek, a w przypadku dostępu do danych osobowych stosownie do wydanych przez Merytorycznych Administratorów Informacji upoważnień do przetwarzania danych osobowych.
7. Użytkownik, przed otrzymaniem loginu i hasła, podpisuje oświadczenie o zapoznaniu się z „Instrukcją zarządzania bezpieczeństwem Zintegrowanego Systemu Zarządzania Oświatą”(wzór oświadczenia stanowi załącznik nr 2 do niniejszego zarządzenia).

Odpowiedzialności

§4

1. **Koordynator jest odpowiedzialny za:**
   1) koordynację i kontrolę poprawności działań mających na celu stworzenie spójnej, zintegrowanej bazy danych, opracowywanie zasad powiązania ze sobą poszczególnych modułów przetwarzających odpowiedni obszar danych i przepływu danych między modułami Systemu;
   2) kierowanie pracami wdrożeniowymi w Wydziale, ZEO i Placówkach odpowiednio do obsługiwanych obszarów danych;
   3) bieżące monitorowanie działania Zintegrowanego Systemu Zarządzania Oświatą oraz analizę potrzeb i oczekiwań Użytkowników w tym obszarze;
   4) współpracę z Gospodarzami, Merytorycznymi Administratorami Informacji oraz Administratorem Systemu;
   5) opracowywanie założeń do modyfikacji i modernizacji Systemu;
   6) organizowanie szkoleń dla Gospodarzy oraz szkoleń i prezentacji dla Użytkowników z zakresu funkcjonowania Zintegrowanego Systemu Zarządzania Oświatą;
   7) kontrolowanie i nadzorowanie wypełniania zbiorów danych Systemu;

8) weryfikację przekazanych przez Gospodarzy uwag merytorycznych o pracy Systemu oraz wniosków o modyfikacje Systemu;
9) opracowywanie procedur korzystania z Systemu.

2. Gospodarz, będący jednocześnie Merytorycznym Administratorem Informacji, jest odpowiedzialny za:

1) merytoryczną koordynację przetwarzania danych przez Użytkowników poszczególnych modułów Systemu;
2) kontrolowanie wypełniania zbiorów danych przez Użytkowników modułów Systemu;
3) terminowość wprowadzania danych do Systemu;
4) poprawność merytoryczną przetwarzanych danych osobowych;
5) zgodność merytoryczną aplikacji przetwarzających dane osobowe z obowiązującymi aktami prawnymi;
6) nadzorowanie przestrzegania zasad ochrony przetwarzanych danych osobowych;
7) zgłaszanie utraty hasła lub/i loginu do Systemu;
8) prowadzenie szkoleń dla nowych użytkowników Systemu, w tym z zakresu ochrony danych osobowych;
9) opracowywanie dla Użytkowników regulaminów, instrukcji;
10) gromadzenie uwag merytorycznych i technicznych o pracy Systemu i przekazywanie ich Koordynatorowi;
11) wnioskowanie do Koordynatora o dokonanie zmian w Systemie usprawniających pracę Użytkowników;
12) informowanie Koordynatora o niewłaściwym wprowadzeniu przez Użytkownika danych powodujących błędne działanie Systemu;
13) wnioskowanie do Koordynatora o cofnięcie uprawnień Użytkownikowi, który wykorzystał je w sposób niewłaściwy;
14) występowanie do Koordynatora o dodanie, usunięcie lub zmianę uprawnień Użytkownika;
15) prowadzenie ewidencji Użytkowników Systemu, która powinna zawierać:
    a) imię i nazwisko
    b) identyfikator Użytkownika
    c) datę przyznania uprawnień
    d) datę cofnięcia uprawnień;
16) udzielanie upoważnienia Użytkownikom z placówki do przetwarzania danych osobowych, wydawanie upoważnień oraz ich ewidencjonowanie;
17) przesyłanie na bieżąco do Referatu ds. ZSZO aktualnych informacji dotyczących listy osób upoważnionych (wzór formularza ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszego zarządzenia);
18) określenie budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe oraz zabezpieczenie tych obszarów w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym;

19) prowadzenie ewidencji pomieszczeń tworzących obszar przetwarzania danych osobowych w danej Placówce, ZEO, Wydziale oraz przesyłanie na bieżąco do Referatu ds. ZSZO aktualnych informacji dotyczących wykazu tych pomieszczeń (wzór formularza wykazu pomieszczeń tworzących obszar przetwarzania danych osobowych stanowi załącznik nr 5 do niniejszego zarządzenia);
20) udzielanie zgody na udostępnianie danych osobowych zgodnie z obowiązującymi przepisami prawa;
21) opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji wraz z załącznikami, zgodnie z ustawą o ochronie danych osobowych, w oparciu o „Instrukcję zarządzania bezpieczeństwem Zintegrowanego Systemu Zarządzania Oświatą" stanowiącą załącznik nr 4 do niniejszego zarządzenia (dotyczy Gospodarza i Merytorycznego Administratora Informacji ZEO i Placówki);
22) uzupełnianie akt osobowych pracowników zatrudnionych przy przetwarzaniu danych osobowych o formularz upoważnienia pracownika do przetwarzania danych osobowych wraz z oświadczeniem poświadczającym zapoznanie się pracownika z „Instrukcją zarządzania bezpieczeństwem Zintegrowanego Systemu Zarządzania Oświatą”;
23) rejestrację zbiorów danych osobowych w Generalnym Inspektoracie Ochrony Danych Osobowych (dotyczy ZEO i Placówek).

3. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za:

1) prowadzenie ewidencji upoważnień pracowników do przetwarzania danych osobowych;
2) nadzorowanie przestrzegania zasad ochrony przetwarzanych danych osobowych;
3) przeprowadzanie okresowych kontroli bezpieczeństwa danych osobowych.

4. Użytkownik jest odpowiedzialny za:

1) ustalenie własnego hasła dostępu do Systemu;
2) zachowanie w tajemnicy haseł chroniących konto Użytkownika;
3) zmianę haseł do posiadanych kont Użytkownika, co najmniej raz na miesiąc oraz w każdym przypadku podejrzenia, iż zostało ujawnione osobie nieuprawnionej;
4) niezwłoczne poinformowanie Gospodarza o utracie hasła;
5) wykorzystywanie posiadanych identyfikatorów Użytkownika zgodnie z indywidualnymi uprawnieniami;
6) prawidłowe korzystanie z Systemu zgodnie z indywidualnymi uprawnieniami;
7) niezwłoczne poinformowanie Gospodarza o nieautoryzowanym dostępie do danych;
8) zgłaszanie awarii Systemu, urządzenia komputerowego, oprogramowania systemowego, sieci komputerowej Gospodarzowi;
9) informowanie Gospodarza o wszelkich nieprawidłowościach działania Systemu;
10) zgłaszanie Gospodarzowi wszelkich zauważonych nieprawidłowości danych przetwarzanych w Systemie;
11) zachowanie szczególnej staranności przy przetwarzaniu danych, aby dane te były:

a) przetwarzane zgodnie z prawem,
b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

5. Administrator Systemu jest odpowiedzialny za:

1) rejestrację Użytkowników w Systemie na wniosek Koordynatora. Rejestracja polega na nadaniu loginu i przydziale hasła pierwotnego, które Użytkownik zmienia przy pierwszym logowaniu do systemu;
2) w przypadku utraty loginu/hasła przydzielenie nowego;
3) nadawanie, zmianę i odebranie indywidualnych uprawnień Użytkownikom na wniosek Koordynatora;
4) nadzór nad procedurą certyfikacji oraz unieważnianiem wydanych certyfikatów;
5) zabezpieczenie Systemu w razie naruszenia ochrony danych osobowych;
6) świadczenie usługi technicznej i administracji technicznej nad infrastrukturą systemową;
7) wprowadzanie zmian i rozwijanie Systemu;
8) usuwanie zaistniałych błędów w Systemie;
9) bieżące administrowanie Systemem w zakresie czynności związanych ze strojeniem Systemu, monitorowaniem wydajności, monitorowaniem logów Systemu, zarządzaniu wzrostem oraz zarządzaniu zmianami.

Konfiguracja i indywidualne uprawnienia użytkownika

§5

1. Gospodarz Placówki bądź ZEO w celu:
   1) utworzenia nowego Użytkownika Systemu;
   2) zmiany upoważnień dla już istniejącego w Systemie Użytkownika;
   3) konieczności odebrania Użytkownikowi dostępu do określonego zbioru danych;
   4) usunięcia Użytkownika

występuje do Koordynatora z prośbą o dokonanie zmiany.

2. Koordynator umieszcza dokładny opis czynności zawartych w ust 1 punkt 1 – 4, które opisuje Procedura konfiguracji Użytkownika, na Portalu Edukacyjnym w zakładce ZSZO – Procedury.

Certyfikacja

§6

1. W celu dokonania certyfikacji Użytkownika należy wypełnić wniosek o certyfikat znajdujący się na stronie internetowej Urzędu Certyfikacyjnego.

2. Koordynator umieszcza dokładny opis czynności niezbędnych do uzyskania certyfikatu zarówno przez Użytkownika będącego dyrektorem (Procedura certyfikacji Użytkownika-dyrektora) jak i przez Użytkownika niebędącego dyrektorem (Procedura certyfikacji pozostałych Użytkowników), na Portalu Edukacyjnym w zakładce ZSZO – Procedury.

§7

Wykonanie zarządzenia powierza się placówkom, ZEO oraz Wydziałowi.

§8

Nadzór nad wykonaniem zarządzenia powierza się Wydziałowi.

§9

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Krakowa
/ - /