Załącznik Nr 4 do Zarządzenia Nr 838/2009
Prezydenta Miasta Krakowa
z dnia 21 kwietnia 2009 r.

Instrukcja zarządzania bezpieczeństwem
Zintegrowanego Systemu Zarządzania Oświatą

1. Ilekroć w niniejszej instrukcji jest mowa o:
   - **„Systemie”** – należy przez to rozumieć Zintegrowany System Zarządzania Oświatą w Krakowie;
   - „**modułach**” – należy przez to rozumieć części Systemu realizujące określoną funkcjonalność;
   - **„dostępie do Systemu”** – należy przez to rozumieć posiadanie konfiguracji tj. indywidualnego loginu i hasła oraz certyfikatu w Systemie;
   - „**organie prowadzącym**” – należy przez to rozumieć Gminę Miejską Kraków;
   - **„Wydziale”** – należy przez to rozumieć Wydział Edukacji Urzędu Miasta Krakowa;
   - **„komórce organizacyjnej Wydziału”** – należy przez to komórkę organizacyjną Wydziału utworzoną w celu koordynacji działań związanych z uruchamianiem Zintegrowanego Systemu Zarządzania Oświatą w Gminie Miejskiej Kraków;
   - **„ZEO”** – należy przez to rozumieć Zespół Ekonomiki Oświaty będący miejską jednostką organizacyjną w Krakowie;
   - „**placówce**” – należy przez to rozumieć przedszkola, szkoły oraz placówki oświatowe prowadzone przez Gminę Miejską Kraków;
   - **„użytkowniku”** – należy przez to rozumieć osobę uprawnioną z placówki, ZEO lub Wydziału mającą indywidualne uprawnienia zapewniające dostęp do Systemu oraz wykonywanie określonych funkcji w Systemie;
   - **„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;
   - **„Administratorze Bezpieczeństwa Informacji”** – należy przez to rozumieć osobę odpowiedzialną za nadzór nad bezpieczeństwem informacji przetwarzanych w Systemie;
   - **„Merytorycznym Administratorze Informacji”** – należy przez to rozumieć osobę odpowiedzialną merytorycznie za przetwarzanie informacji w Systemie oraz w dyspozycji której znajdują się te informacje.

2. Zasady ochrony danych osobowych:
   1) Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie wydane przez dyrektora placówki/ZEO.
   2) Ewidencję upoważnień użytkowników Systemu w danej placówce/ZEO, prowadzi Merytoryczny Administrator Informacji. Ewidencja powinna zawierać:
      a) imię i nazwisko
      b) identyfikator użytkownika
      c) datę przyznania uprawnień
      d) datę cofnięcia uprawnień

3) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu loginu użytkownika i właściwego hasła.
4) Każdy użytkownik Systemu przetwarzający dane osobowe ma ustalony indywidualny, niepowtarzalny identyfikator i hasło dostępu.
5) Merytoryczny Administrator Informacji przed przekazaniem użytkownikowi identyfikatora i hasła przeprowadza szkolenie z zakresu bezpieczeństwa danych w Systemie.
6) Login osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić hasło oraz podjąć inne stosowne działania celem zapobieżenia dalszego dostępu tej osoby do danych.
7) Hasło użytkownika winno być zmieniane co 30 dni.
8) Hasło użytkownika nie może być zapisywane w miejscach dostępnych dla osób nieuprawnionych. Użytkownik nie może udostępnić loginu, hasła i stanowiska roboczego osobom nieuprawnionym.
9) Wszystkie komputery na których przetwarzane są dane osobowe powinny być zabezpieczone hasłem.
10) Pracownicy nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym.
11) Ekrany monitorów stanowisk, na których przetwarzane są dane osobowe, powinny być automatycznie wyłączane po upływie maksimum 5 minut czasu nieaktywności użytkownika.
12) Użytkownik ma obowiązek wylogowania się z systemu przy rozpoczęciu dłuższej nieobecności na stanowisku pracy lub zakończeniu tej pracy. Stanowisko komputerowe z uruchomionym systemem nie może pozostać bez kontroli pracującego na nim pracownika.
13) Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby nieuprawnione. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.
14) Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich zatrudnionych w sposób uniemożliwiający dostęp do nich osób trzecich.
15) Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami sieci zasilającej.
16) Celem przeciwdziałania zagrożeniom ze strony wirusów komputerowych i innych zagrożeń, które są związane z podłączeniem sieci lokalnej z publiczną:
    a) komputery z dostępem do Internetu muszą być zabezpieczone za pomocą oprogramowania antywirusowego;
    b) zbiory danych będące w bezpośrednim użytkowaniu winny być sprawdzane na obecność wirusów komputerowych co najmniej raz w tygodniu lub w razie potrzeby częściej;
17) Urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe należy pozbawić tych danych przed ich przekazaniem innemu podmiotowi. Nośniki danych

zawierające dane osobowe winny być likwidowane przez uszkodzenie w sposób uniemożliwiający ich odczytanie. Naprawę wymienionych urządzeń należy wykonać pod nadzorem osoby upoważnionej przez Merytorycznego Administratora Informacji lub jeśli jest to możliwe, pozbawić je danych osobowych przed wydaniem ich do naprawy.

18) Korzystającym z systemu informatycznego w Urzędzie zabrania się:
    a) udostępniania stanowiska pracy oraz istniejących w nich danych osobom nieupoważnionym;
    b) udostępniania osobom nieuprawnionym programów komputerowych;
    c) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna;
    d) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne;
    e) samowolnego instalowania i używania programów komputerowych; programy komputerowe instalowane są przez administratora systemu lub za jego zgodą przez inną upoważnioną osobę;
    f) używania nośników danych udostępnionych przez osoby nieuprawnione;
    g) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy te nośniki przeskanować programem antywirusowym; jeżeli program antywirusowy nie jest zainstalowany na danej stacji roboczej należy to zrobić na innym stanowisku;
    h) wykorzystywania sieci komputerowej w celach innych, niż wyznaczone przez administratora danych osobowych.

3. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:
    1) stwierdzono nieuprawniony dostęp do Systemu;
    2) stwierdzono naruszenie zabezpieczenia Systemu;
    3) stwierdzono naruszenie fizycznych lub elektronicznych zabezpieczeń pomieszczeń, w których przechowywany jest sprzęt komputerowy używany do przetwarzania danych osobowych;
    4) stwierdzono obecność wirusów komputerowych lub szkodliwego oprogramowania;
    5) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

4. W przypadku stwierdzenia bądź podejrzenia naruszenia ochrony danych osobowych w Systemie każdy użytkownik zobowiązany jest do:

1) niezwłocznego poinformowania o tym fakcie bezpośredniego przełożonego, Administratora Systemu oraz Administratora Bezpieczeństwa Informacji placówki/ZEO, który zgłasza ten fakt do Koordynatora Systemu.
2) Sporządzenia notatki służbowej z opisem sytuacji wskazującej na naruszenie zabezpieczeń systemu informatycznego i przekazuję ją Administratorowi Bezpieczeństwa Informacji placówki/ZEO.

5. Merytoryczny Administrator Informacji, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:
   1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu;
   2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania;
   3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.;
   4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.
      a) fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
      b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych;
      c) zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu;
   5) szczegółowej analizy stanu Systemu w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;
   6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

6. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
7. Administrator Bezpieczeństwa Informacji placówki/ZEO przeprowadza postępowanie wyjaśniające w celu określenia przyczyn naruszenia danych osobowych lub podejrzenia takiego naruszenia oraz przekazuje informacje w formie pisemnej wraz z zaleceniami jakie kroki należy podjąć, aby wyeliminować podobne zdarzenia w przyszłości Koordynatorowi Systemu.

8. Koordynator Systemu o całości zajścia informuje Głównego Administratora Bezpieczeństwa Informacji.
9. Jeżeli przyczyną zdarzenia był błąd użytkownika Systemu należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
10. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.