Zarządzenie nr 178 / VI / 2012
Burmistrza Miastka
z dnia 4 lipca 2012 r.

w sprawie : wprowadzenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Miastku.

Na podstawie art.31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j. t. Dz. U. z 2001 r. Nr 142, poz.1591 z późn. zm.) **zarządzam**, co następuje :

§ 1.

Z dniem 15 lipca 2012 r. w Urzędzie Miejskim w Miastku wprowadzam instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Wykonanie zarządzenia powierzam Sekretarzowi Miastka.

§ 3.

Zarządzenie wchodzi w życie z dniem podjęcia

Projekt zarządzenia
opiniuję pod względem formalno-prawnym
pozytywnie \ ~~negatywnie~~

Miastko, dnia 4 lipca 2012r.

Marek Kobyłecki
RADCA PRAWNY

BURMISTRZ
MIASTKA

Roman Ramion

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Rozdział I.
CZĘŚĆ OGÓLNA

§1-

Instrukcja określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Miastku.

§2.

Ilekroć w niniejszej instrukcji mowa o:
1) Urzędzie - należy rozumieć przez to Urząd Miejski w Miastku,
2) Administratorze Danych Osobowych - należy rozumieć przez to Burmistrza Miastka,
3) Administratorze Bezpieczeństwa Informacji - należy rozumieć przez to osobę wyznaczoną przez Administratora Danych Osobowych do pełnienia tej funkcji,
4) użytkowniku danych osobowych - należy rozumieć każdego pracownika, który wykonując czynności służbowe przetwarza dane osobowe, tzn. wykonuje na nich jakiekolwiek operacje, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie.
5) systemie informatycznym - należy rozumieć przez to system informatyczny wdrożony w Urzędzie Miejskim w Miastku.

§3.

Informacje zawarte w prowadzonych w Urzędzie różnego rodzaju rejestrach, ewidencjach, kartotekach, wykazach oraz w systemach informatycznych dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, pozwalające na bezpośrednie lub pośrednie określenie tożsamości tej osoby uznaje się za dane osobowe.

§4.

1. Do obowiązków Administratora Bezpieczeństwa Informacji należy:
   1) czuwanie nad wdrażaniem w Urzędzie niniejszej instrukcji oraz dbanie o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych,
   2) identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych,
   3) określanie potrzeb w zakresie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe,
   4) nadawanie identyfikatorów użytkownikom danych osobowych,
   5) zabezpieczenie i kontrolowanie prawidłowości przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,
   6) pozbawianie zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie urządzeń lub nośników, które przeznaczone są do likwidacji,
   7) instalowanie zabezpieczeń w systemach informatycznych,

8) wyrejestrowywanie i rejestrowanie z systemu użytkowników w czasie instalowania oraz modyfikacji systemu,
9) przydzielanie uprawnień do poszczególnych systemów,
10) wykonywanie kopii awaryjnych danych z serwera, właściwe przechowywanie nośników, sprawdzanie poprawności zapisu oraz ich likwidowanie,
11) dokonywanie wyboru lub migracji do technologii minimalizującej zagrożenia uzyskania dostępu do sieci osobom nieupoważnionym,
12) nadzorowanie procesu monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nie upoważnionych,
13) prowadzenie ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych.

§5.

1. Dostęp pracowników do obsługi systemu informatycznego przetwarzającego dane osobowe oraz urządzeń wchodzących w jego skład możliwy jest wyłącznie na podstawie upoważnienia wydanego przez Administratora Danych Osobowych.
2. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.
3. Oświadczenia o zachowaniu tajemnicy służbowej, o której mowa w ust. 2 przechowywane są w aktach osobowych pracowników.
4. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych.

§6.

1. Udostępnianie danych osobowych ze zbioru danych osobom lub podmiotom uprawnionym do ich otrzymania odbywać się może na pisemny umotywowany wniosek.
2. Decyzję o udostępnieniu danych osobowych podejmuje Administrator Danych Osobowych, po uzyskaniu opinii wydziału merytorycznego.
3. Po otrzymaniu zgody od Administratora Danych Osobowych, dane do udostępnienia przygotowuje użytkownik danych osobowych. Użytkownik jest zobowiązany do odnotowania w systemie informatycznym informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.

Rozdział II. ZASADY PRZYDZIAŁU HASEŁ DLA UŻYTKOWNIKÓW

§7.

1. Dla każdego użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe przydziela się odrębny identyfikator i hasło oraz uprawnienia w systemie zgodnie z zakresem obowiązków.
2. Przyznany użytkownikom identyfikator jest niezmienny, natomiast użytkownik jest zobowiązany do zmiany hasła raz na miesiąc.
3. Za przydział i rejestrację identyfikatorów dostępu do systemów przetwarzających dane osobowe odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
4. Identyfikatory pracowników oraz hasła dostępu do systemu informatycznego stanowią tajemnicę służbową.
5. Użytkownik po otrzymaniu indywidualnego identyfikatora oraz hasła powinien je zapamiętać. Nie wolno ich zapisywać w miejscach, które umożliwiłyby osobom trzecim zapoznanie się z nimi.
6. W przypadku, gdy dane osobowe przetwarzane są w programach typu Office na pojedynczym komputerze, użytkownik danych osobowych zobowiązany jest zabezpieczyć plik hasłem.

Rozdział III.

PROCEDURY ROZPOCZĘCIA I ZAKOŃCZENIA PRACY PRZY KOMPUTERZE

§8.

1. Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną.
2. Użytkownicy uzyskują bezpośredni dostęp do danych w aplikacji po podaniu identyfikatora i właściwego hasła.
3. Kończąc pracę użytkownik powinien:
   1) zamknąć program oraz wyjść z systemu i wyłączyć komputer wraz z drukarką,
   2) sprawdzić, czy pozostawione stanowisko nie stwarza jakichkolwiek zagrożeń i czy są prawidłowo zabezpieczone przed uruchomieniem ich przez osoby postronne.
   3) sprawdzić czy w napędach komputera nie pozostały nośniki zawierające dokumenty lub informacje zawierające dane osobowe, niejawne lub inne do których wgląd modą mieć jedynie wybrani pracownicy urzędu.
4. Wszystkie zauważone usterki i mankamenty na stanowisku użytkownik winien natychmiast zgłosić bezpośredniemu przełożonemu, odpowiednim służbom konserwacyjnym oraz Administratorowi Bezpieczeństwa Informacji.
5. W przypadku chwilowego opuszczenia stanowiska pracy należy wylogować się z systemu informatycznego.

§9.

1. W przypadku stwierdzenia przez użytkownika danych osobowych naruszenia zabezpieczeń systemu informatycznego, na które mogą wskazywać:
   1) stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),
   2) różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych opcjach),
   3) różnica w zawartości zbioru danych osobowych (np. brak lub nadmiar danych), jest on zobowiązany niezwłocznie powiadomić o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji, a w przypadku ich nieobecności - bezpośrednio Administratora Danych Osobowych.
2. Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba powinna w pierwszej kolejności:
   1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
   2) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,
   3) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
   4) niezwłocznie podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji,
   5) przywrócić normalny stan działania systemu.
3. Po wyeliminowaniu bezpośredniego zagrożenia Administrator Bezpieczeństwa Informacji ma obowiązek przeprowadzić analizę stanu systemu informatycznego, a w szczególności sprawdzić:
   1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   2) zawartość zbioru danych osobowych,

3) sposób działania programu,
4) jakość komunikacji w sieci telekomunikacyjnej,
5) obecność wirusów komputerowych.

Rozdział IV.
METODY I CZĘSTOTLIWOŚĆ TWORZENIA KOPII AWARYJNYCH ORAZ SPOSÓB I CZAS ICH PRZECHOWYWANIA

§10.

1. Dane zgromadzone w pamięciach komputerów powinny być zabezpieczone przed ich utratą przez tworzenie ich kopii awaryjnych w cyklach:

   - codziennym,
   - tygodniowym,
   - miesięcznym.

2. Za archiwizację danych przechowywanych w pamięci serwerów sieciowych odpowiedzialny jest Administrator Bezpieczeństwa Informacji. W cyklu codziennym należy archiwizować zmiany, a w cyklu tygodniowym całą zawartość baz danych przechowywanych w pamięci serwerów sieciowych. Zarchiwizowane dane należy przechowywać w odpowiednio chronionym i zabezpieczonym pomieszczeniu, poza pomieszczeniem w którym umieszczony jest serwer sieciowy.
3. Kopie zapasowe danych z serwera archiwizowane w cyklu miesięcznym należy przechowywać w odpowiednio zabezpieczonym pomieszczeniu innym niż pomieszczenie w którym przechowywane są dane z cykli codziennych i tygodniowych, poza pomieszczeniem w którym znajduje się serwer. Za archiwizowanie danych z pamięci serwerów w cyklu miesięcznym odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

Rozdział V.

SPOSÓB i CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI

§11.

1. Nośniki informatyczne, wydruki zawierające dane osobowe oraz kopie awaryjne, o których mowa w § 10 ust. 2-4, przechowywać należy w wyznaczonych pomieszczeniach, w zamkniętych szafach.
2. Kopie zapasowe, o których mowa w § 10 ust. 2 i 3 powinny być przechowywane przynajmniej 7 dni.
3. Kopie zapasowe, o których mowa w § 10 ust. 4 winny być przechowywane przynajmniej przez 6 miesięcy.
4. Użytkownicy na koniec każdego okresu, o którym mowa w ust. 2 i 3, winni dokonać analizy przydatności kopii awaryjnych.
5. Za wydruki zawierające dane osobowe odpowiedzialni są użytkownicy danych osobowych, którzy je wykonali. Wydruki te winny być przechowywane zgodnie z terminami określonymi w instrukcji kancelaryjnej dla urzędów gmin.
6. Każdy użytkownik ma obowiązek pozbawiania zapisu danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych oraz do pozbawiania zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie nośników, które przeznaczone są do likwidacji.

Rozdział VI.
DOKONYWANIE PRZEGLĄDÓW I KONSERWACJI SYSTEMU I ZBIORU DANYCH OSOBOWYCH

§12.

1. Raz na kwartał Administrator Bezpieczeństwa Informacji lub wyznaczona przez niego osoba, dokonuje przeglądu i konserwacji systemu informatycznego i zbioru danych osobowych.
2. W przypadku konieczności oddania sprzętu zawierającego dane osobowe do naprawy na zewnątrz, Administrator Bezpieczeństwa Informacji zobowiązany jest do usunięcia zapisanych danych. W przypadku gdy nie można tych danych usunąć, naprawa sprzętu winna być dokonywana pod nadzorem Administratora Bezpieczeństwa Informacji.

Rozdział VII.
SPOSÓB POSTĘPOWANIA W ZAKRESIE ZWIĘKSZENIA BEZPIECZEŃSTWA SIECI KOMPUTEROWEJ

§13.

1. Ogranicza się w Urzędzie obieg dyskietek i innych nośników informatycznych poprzez ich ostemplowanie pieczęcią Urzędu Miejskiego w Miastku.
2. Wprowadza się zakaz obiegu nośników nie oznakowanych w sposób, o którym mowa w ust. 1, a wszystkie nośniki przychodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu z nich danych po uprzednim sprawdzeniu programem antywirusowym u informatyków Urzędu.

§14.

Systemy do przetwarzania danych osobowych są zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu, przez odpowiednie oprogramowanie.

§15.

Zabrania się:
1) udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,
2) wykorzystywania sieci komputerowej w celach innych niż służbowych,
3) samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji),
4) trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie,
5) publicznego rozpowszechniania programów komputerowych lub ich kopii,
6) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
7) udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu,
8) wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez wyraźnego upoważnienia Administratora Bezpieczeństwa Informacji,
9) używania prywatnych skrzynek mailowych działających na innych serwerach niż urzędowy bez uzgodnienia z Administratorem Bezpieczeństwa Informacji,
10) uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści,
11) kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody Administratora Danych Osobowych.

Polityka bezpieczeństwa.

1. **Wykaz budynków i pomieszczeń Urzędu Miasta w Miastku tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego**

Urząd Miejski w Miastku

Lp.	Numer pomieszczenia	Nazwa Wydziału, nazwa pomieszczenia
PARTER		
1	1	Wymiar Podatków
2	2	Kierownik Referatu Podatków
3	3	Windykacja Podatkowa
4	4	Kasa
5	7	Biuro Obsługi Klienta
6	9	Biuro Rady
7	11	Urząd Stanu Cywilnego
I PIĘTRO		
8	12-15	Wydział Rolnictwa Gospodarki Nieruchomościami i Ochrony Środowiska
9	16-18	Wydział Infrastruktury Technicznej
10	19	Sekretariat Burmistrza
11	20-22	Księgowość
12	23-25	Wydział Oświaty Kultury i Sportu
13	25-28	Wydział Organizacyjny
II PIĘTRO		
14	49	Referat Spraw Obywatelskich i Działalności Gospodarczej
15	48, 47, 45	Wydział Rozwoju Lokalnego i Promocji
III PIĘTRO		
16		Straż Miejska

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru danych osobowych	NAZWA PROGRAMU
1	* Ewidencja Ludności, Rejestr Wyborców, * Księgowość: księgowość budżetowa, budżet zadaniowy, kadry i płace środki trwałe, księgowość podatkowa z windykacją, obsługa kasy, * Ewidencje i rejestry: nieruchomości, gospodarstw, lasów, gruntów, budynków, działalności gospodarczej, wydawanych zezwoleń, * Naliczanie podatków, opłat za użytkowanie wieczyste gruntów, * Pomoc społeczna: stypendia oświatowe, dodatki mieszkaniowe	Radix
2	USC	Technika Gliwice
3	Zintegrowany system zarządzania w oświacie (kadry, płace, FK)	Vulcan
4	Arkusz organizacyjny	ProgMan
5	Elektroniczny obieg dokumentów	AlfaTV

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

a) Moduły sytemu RADIX, USC Vulcan przechowywane są na sieciowych serwerach danych pracujący w oparciu o MsSql, MySql, DBF. Dostęp do danych przyznawany jest na podstawie utworzonych w systemie kont użytkowników. Pracownicy odpowiedzialni za przetwarzanie określonych danych osobowych mają dostęp do odpowiednich zbiorów danych przypisany do kont użytkownika
na które się logują. Pozostali użytkownicy systemu nie mają dostępu do baz zawierających dane osobowe.

4. Sposób przepływu danych pomiędzy poszczególnymi systemami.

W Urzędzie Miejskim w Miastku, jedynie moduły systemu RADIX korzystają ze wspólnych baz danych. Posiadają one wspólne bazy danych znajdujące się w tym samym folderze. Dostęp do danych jest współdzielony i każdy z modułów systemu RADIX, korzysta z danych w określonym dla siebie zakresie .

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Wszystkie programy wykorzystywane do przetwarzania danych osobowych posiadają własny system identyfikacji użytkowników. Każdy użytkownik przetwarzający dane osobowe posiada swój własny identyfikator utworzony w programie, w którym przetwarza dane. Identyfikator taki zabezpiecza dane przed niepowołanym dostępem. Poszczególne systemy za pomocą mechanizmu rejestracji zapamiętują informacje związane z czasem pracy użytkowników. Pracownicy UM w Miastku mają przydzielone zakresy obowiązków zgodnie, z którymi odpowiadają za przetwarzanie określonych baz danych osobowych. W każdym przypadku jest wyznaczona jedna osoba (oraz osoby zastępujące ją na czas nieobecności) odpowiedzialna za konkretny zbiór danych, posiadająca niepowtarzalny identyfikator, który umożliwia rozliczalność wprowadzanych zmian.

BURMISTRZ
MIASTKA
Roman Ramion