Zarządzenie nr 403/2010
Burmistrza Toszka

z dnia 30 listopad 2010 r

w sprawie : wprowadzenia do użytku służbowego Instrukcji dotyczących ochrony danych osobowych przetwarzanych w Urzędzie Miejskim w Toszku

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r o samorządzie gminnym (t.j. Dz.U. Nr 142 , poz. 1591 z późn.zm.) oraz § 3 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 służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024)

zarządzam , co następuje :

1. Wprowadzić w Urzędzie Miejskim w Toszku „Politykę bezpieczeństwa oraz instrukcję określającą sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Toszku" w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia .

2. Wprowadzić w Urzędzie Miejskim w Toszku „Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Toszku „ w brzmieniu załącznika nr 2 do niniejszego zarządzenia.

3. Zobowiązuje się pracowników Urzędu Miejskiego w Toszku do przestrzegania postanowień dokumentów , o których mowa w ust. 1 i2 .

4. Tracą moc :
1) zarządzenie nr 2 /99 Burmistrza Miasta i Gminy Toszek z dnia 14 stycznia 1999 r w sprawie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Toszku .
2) zarządzenie nr 3/99 Burmistrza Miasta i Gminy Toszek z dnia 14 stycznia 1999 r w sprawie postępowania w przypadku naruszenia ochrony danych osobowych dla osób zatrudnionych przy przetwarzaniu danych osobowych .
3) decyzja nr 1/2004 Burmistrza Toszka z dnia 26 maja 2004 r w sprawie wprowadzenia do użytku służbowego Instrukcji dotyczących danych osobowych oraz polityki bezpieczeństwa w Urzędzie Miejskim w Toszku.

5. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Bezpieczeństwa Systemów Informatycznych.

6. Zarządzenie wchodzi w życie z dniem podpisania.

wz. BURMISTRZA
Maria [illegible] Kowalska
Z-ca Burmistrza

RADCA PRAWNY
mgr Mariola Hajduk

Załącznik nr 1
Do zarządzenia nr 403/2010
Burmistrza Toszka
z dnia 30.11.2010

Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemami Informatycznymi w Urzędzie Miejskim w Toszku

ROZDZIAŁ 1
Postanowienia ogólne.

§ 1

Instrukcja Zarządzania Systemami Informatycznymi jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania Systemami Informatycznymi Urzędu Miejskiego w Toszku. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, w szczególności zaś osoby pełniące funkcje:

1. administratora bezpieczeństwa informacji w Urzędzie;
2. administratorów systemów informatycznych wyznaczonych w Urzędzie Miejskim w Toszku;

§ 2

Określenia i skróty użyte w Instrukcji oznaczają:

1. Administrator Danych Osobowych – Burmistrz Toszka, zwany dalej Administratorem.
2. ABI - Administrator Bezpieczeństwa Informacji – osoba wyznaczona przez Administratora, w rozumieniu art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.), dalej zwana Ustawą.
3. ASI - Administratorzy Systemów Informatycznych – pracownicy wyznaczeni przez Burmistrza odpowiedzialni za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązani do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.
4. Użytkownik systemu – osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu.
5. Przełożony użytkownika, zwany dalej przełożonym – Kierownik Biura, Kierownik USC, - osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników.
6. Hasło – ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
7. Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
8. Sieć LAN/WAN – sieć lokalna/rozległa umożliwiająca połączenie systemów informatycznych Urzędu Miejskiego w Toszku przy wykorzystaniu specjalistycznych dedykowanych urządzeń i sieci telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).
9. Dane sensytywne - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym.
10. Rejestr udostępnionych danych osobowych, zwany dalej Rejestrem – rejestr, w którym odnotowywane są informacje o odbiorcach danych z systemu/aplikacji, prowadzony dla danego systemu/aplikacji.

ROZDZIAŁ 2
Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych

§ 3

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych zapoznaje się z:
   a) niniejszą instrukcją,
   b) procedurami określonymi przez Administratora Danych Osobowych.
2. Podstawą nadania uprawnień jest wniosek przełożonego.

§ 4

1. Opis procedury nadawania/odbierania uprawnień dostępu do lokalnej sieci komputerowej przedstawiony jest poniżej. Stosowany w Urzędzie Miejskim w Toszku schemat uprawnień dostępu do sieci LAN/WAN zakłada, iż użytkownicy uzyskują dostęp do sieci na z góry zdefiniowanym poziomie użytkownika w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.
2. Przełożony użytkownika:
   a) wnioskuje o nadanie/odebranie pracownikowi uprawnień do przetwarzania danych w systemach/aplikacjach eksploatowanych w sieci LAN/WAN Urzędu Miejskiego w Toszku w związku z wykonywanymi przez niego zadaniami,
   b) zgłasza do ASI lub ABI potrzebę nadania/odebrania uprawnień w systemie informatycznym na wymaganym poziomie, w formie pisemnej lub ustnej w sytuacji natychmiastowego odebrania uprawnień.
3. ASI/ABI na podstawie otrzymanego pisma/polecenia wykonuje:
   a) rejestruje/usuwa użytkownika w systemie i nadaje mu wymagane uprawnienia,
   b) informuje w formie elektronicznej/ustnej, przełożonego użytkownika oraz ABI/ASI o fakcie nadania/odebrania uprawnień. W przypadku nadania uprawnień, informuje dodatkowo o założonym koncie wnioskowanym dla użytkownika i nadanych uprawnieniach,
   c) w przypadku, gdy nadanie pracownikowi wymaganych uprawnień może grozić naruszeniem standardów bezpieczeństwa systemów/aplikacji pracujących w sieci, ASI/ABI informuje przełożonego użytkownika w formie elektronicznej o tym zagrożeniu i wstrzymuje proces nadawania uprawnień. Przełożony użytkownika ponownie może wnioskować o przyznanie pracownikowi zmodyfikowanych uprawnień, które nie stanowią zagrożenia naruszenia bezpieczeństwa, a jego wniosek musi zostać zaakceptowany przez ABI/ASI.
4. Użytkownik, po otrzymaniu od ASI/ABI informacji o założonym koncie z wymaganymi uprawnieniami, wykonuje:
   a) loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,
   b) przy pierwszym logowaniu się do systemu/aplikacji, użytkownik musi zmienić nadane mu przez ASI/ABI hasło.
5. Powyższy schemat nadania/odebrania uprawnień dostępu do systemów/aplikacji eksploatowanych w sieci LAN/WAN należy stosować również w przypadku wymaganej zmiany w istniejących uprawnieniach użytkownika.

§ 5

1. Powyższe zasady nadawania/odbierania uprawnień dostępu do wszystkich systemów/aplikacji eksploatowanych w Urzędzie Miejskim w Toszku obowiązują wszystkich pracowników.
2. W przypadku gdy system/aplikacja nie posiada wbudowanych mechanizmów kontroli dostępu, wówczas należy niezwłocznie rozbudować taki system/aplikacje o te mechanizmy, a do czasu wdrożenia takich mechanizmów należy zaimplementować ograniczenia dostępu na poziomie systemu operacyjnego, bądź ograniczenia proceduralne.

ROZDZIAŁ 3
Metody i środki uwierzytelnienia w systemach informatycznych

§ 6

1. Naczelną zasadą bezpieczeństwa systemów/aplikacji i sieci IT jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników systemów/aplikacji (w tym sieci LAN/WAN) ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 7

1. W systemach/aplikacjach informatycznych Urzędu Miejskiego w Toszku stosuje się uwierzytelnienie dwustopniowe, na poziomie:
   a) dostępu do sieci LAN/WAN,
   b) dostępu do systemu/aplikacji.
2. Do uwierzytelnienia użytkownika w systemie/aplikacji na obu poziomach używa się identyfikatorów, haseł możliwe jest karty inteligentnej.
   a) stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach i sieciach teleinformatycznych Urzędu Miejskiego w Toszku,
   b) zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi (nie dopuszcza się, aby użytkownik korzystał z kont: administrator, gość, a także z konta innego użytkownika),
   c) ograniczenie dostępu do informacji jedynie do kręgu użytkowników uprawnionych (autoryzowanych) wymaga przyjęcia odpowiednio dobranej polityki stosowania haseł.
3. W Urzędzie Miejskim w Toszku, stosuje się poziom bezpieczeństwa przetwarzania danych adekwatnie do klasyfikacji tych danych w systemach/aplikacjach. W związku z powyższym, obowiązujące są trzy poziomy bezpieczeństwa:
   a) poziom podstawowy - dla systemów/aplikacji, w których nie są przetwarzane dane osobowe sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi się składać z co najmniej 6-ciu znaków,
   b) poziom podwyższony - dla systemów/aplikacji, w których są przetwarzane dane sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi składać się z co najmniej 8 znaków, i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   c) poziom wysoki - dla systemów/aplikacji, w których są przetwarzane dane sensytywne oraz co najmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych jest połączone z siecią publiczną. Wówczas Administrator danych musi stosować środki co najmniej 3 haseł przed dostępem do sieci WAN lub kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania.
4. Hasło dostępu do sieci LAN/WAN musi składać się z minimum 6 znaków.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych bezpośrednio kojarzących się z użytkownikiem.
6. Hasło nie może być ujawnione innej osobie nawet po utracie ważności hasła.

7. System automatycznie powinien wymuszać zmianę hasła nie rzadziej, niż jeden raz w miesiącu. Hasło musi być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia.

§ 8

1. Procedura zarządzania środkami uwierzytelniania
   a) ASI/ABI nadaje hasło dostępu do systemu/aplikacji lub sieci LAN/WAN dla nowego użytkownika albo dla użytkownika, który zapomniał swojego ostatniego hasła,
   b) użytkownik systemu/aplikacji niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ASI/ABI. System automatycznie wymusza na użytkowniku zmianę nadanego przez administratora hasła przy pierwszym logowaniu,
   c) użytkownik systemu w dowolnym momencie może zmienić swoje hasło dostępu do systemu/aplikacji,
   d) obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu,

ROZDZIAŁ 4
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

§ 9

1. Procedura rozpoczęcia pracy
   a) uruchomić komputer wchodzący w skład systemu informatycznego, podłączony fizycznie do sieci lokalnej i zalogować się podając własny identyfikator i hasło dostępu,
   b) uruchomić wybrany system/aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane),
   c) zalogować się do systemu/aplikacji w sposób analogiczny do przedstawionego powyżej.
2. Procedura zawieszenia pracy w systemie/aplikacji. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie komputera. Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem lub wylogowania się z systemu.
3. Procedura zakończenia pracy w systemie
   a) zamknąć system/aplikację,
   b) zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
   c) wyłączyć UPS
   d) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.
4. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

ROZDZIAŁ 5
Procedury tworzenia kopii zapasowych danych

§ 10

1. W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych Urzędu Miejskiego w Toszku, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach danych Urzędu Miejskiego w Toszku w oparciu o architekturę klient – serwer. Wynika stąd praktyka przetwarzania danych w bazach danych na dedykowanych dla systemu/aplikacji serwerach.
2. Jeśli stosowane dotychczas rozwiązania nie są zgodne z architekturą klient – serwer, to należy zapewnić możliwość przechowywania gromadzonych za ich pomocą danych na wyznaczonym serwerze plików.
3. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Urzędu Miejskiego w Toszku, stanowią jedynie końcówki klienckie systemu komputerowego.
4. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach.
5. W szczególnych przypadkach, za zgodą ABI/ASI, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych niepodłączonych do sieci LAN/WAN Urzędu Miejskiego w Toszku. W takich przypadkach obowiązek wykonania kopii bezpieczeństwa aplikacji oraz codziennego wykonywania kopii bezpieczeństwa bazy danych oraz ich bezpiecznego przechowywania (zgodnie z zasadami opisanymi w poniższym § 11 ust.3), spoczywa bezpośrednio na użytkowniku danej aplikacji.
6. Opisywana tu zasada przetwarzania danych wpływa bezpośrednio na zagadnienia związane z tworzeniem kopii bezpieczeństwa systemów.

§ 11

1. Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są:
   a) w cyklu dobowym (w godzinach nocnych) za pomocą aplikacji archiwizujących dane do postaci tzw. kopii przyrostowych (zawierających zapis jedynie tych informacji, które podczas ostatniej doby uległy zmianie),
   b) w cyklu tygodniowym, podobnie przy użyciu oprogramowania aplikacji archiwizujących, tworzone są pełne kopie baz danych oraz aplikacji,
   c) w cyklu miesięcznym tworzony jest „ręczny", pełny backup systemu (łącznie z kopią systemu operacyjnego serwera).
2. ASI/ABI sprawuje nadzór nad wykonywaniem ww. kopii zapasowych oraz weryfikuje ich poprawność.
3. Zasady przechowywania kopii
   a) kopie zapasowe zbioru danych oraz oprogramowania i narzędzi programistycznych zastosowanych do przetwarzania danych są przechowywane w przeznaczonej do tego celu metalowej szafie, znajdującej się w wyznaczonym pomieszczeniu w Biurze Informatyków.
   b) dostęp do metalowej szafy mają tylko upoważnieni pracownicy, tj. ASI/ABI.

ROZDZIAŁ 6

Przechowywanie nośników informacji zawierające dane oraz kopii zapasowych

§ 12

1. Elektroniczne nośniki informacji
   a) dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (np. dyskietkach, dyskach magnetooptycznych, taśmach magnetycznych czy dyskach twardych) są własnością Urzędu Miejskiego w Toszku,
   b) wyżej wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych,
   c) po zakończeniu pracy przez użytkowników systemu/aplikacji, ww. elektroniczne nośniki informacji są przechowywane w meblach biurowych ze sprawnym zamknięciem lub w kasetkach,
   d) elektroniczne nośniki informacji, o których mowa powyżej, powinny być oznaczone w sposób umożliwiający ich identyfikację.
2. Przekazywanie i niszczenie elektronicznych nośników informacji
   a) elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez Administratora Danych Osobowych,
   b) dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone przed odczytem (minimum hasłem),
   c) dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych,
   d) przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez ASI/ABI oraz właściwych użytkowników. Protokół zatwierdzony przez przełożonego użytkownika należy przesłać do ABI/ASI.

ROZDZIAŁ 7
Środki ochrony systemów informatycznych

§ 13

1. Poniżej przedstawiono zasady ochrony systemów przetwarzania danych przed tzw. „szkodliwym oprogramowaniem" oraz próbami penetracji przez osoby nieuprawnione.
2. Ochrona antywirusowa
   a) za ochronę antywirusową odpowiada ASI/ABI,
   b) czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI/ABI, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego,
   c) oprogramowanie antywirusowe jest instalowane centralnie na serwerze, oraz na wszystkich stanowiskach komputerowych podłączonych do sieci,
   d) aktualizacja oprogramowania antywirusowego odbywa się nie rzadziej niż raz w tygodniu, w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci,
   e) instalacja oprogramowania antywirusowego oraz jego aktualizacja na komputerach niepodłączonych do sieci, odbywa się nie rzadziej niż raz w tygodniu i jest wykonywana przy zastosowaniu nośników zewnętrznych przez wyznaczonych pracowników Biura Informatyki,

f) użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.

§ 14

1. ASI/ABI jest odpowiedzialny za aktywowanie i poprawną konfigurację specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej i sieci rozległej (LAN/WAN),
   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
2. Ochrona przed awarią zasilania
   a) system, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
   b) dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu,
   c) dane osobowe przetwarzane z wykorzystaniem serwera w wewnętrznych sieciach teleinformatycznych należy zabezpieczać przed zanikiem napięcia wykorzystując centralny UPS i generator prądu.

ROZDZIAŁ 8
Monitorowanie dostępu do danych

§ 15

1. Dla każdego systemu, w którym przetwarzane są dane osobowe, prowadzony jest Rejestr, w którym odnotowywane są informacje o odbiorcach danych z tego systemu (o ile występuje dla danego systemu proces udostępniania danych osobom wymienionym w § 15 ust.2).
2. Odbiorcą danych jest każdy, komu udostępnia się dane
   a) osoby, której dane dotyczą,
   b) podmiotu, któremu powierzono przetwarzanie danych,
   c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o
   a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   b) zakresie udostępnianych danych,
   c) dacie udostępnienia.
4. Obowiązek odnotowania ww. informacji w Rejestrze spoczywa na użytkowniku systemu udostępniającemu dane.
5. Odnotowanie informacji w Rejestrze powinno nastąpić niezwłocznie po udostępnieniu danych.
6. Na podstawie art. 29 Ustawy o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) udostępnienie danych osobowych może nastąpić w następujących przypadkach:
   a) w celu innym niż włączenie danych do zbioru - Administrator udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   b) dane osobowe, z wyłączeniem danych sensytywnych mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w

§ 15 ust 6 lit a), jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

c) dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

7. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
8. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnionych danych są zamieszczane w raporcie z Rejestru, a raport przekazywany tej osobie.
9. Nadzór nad prawidłowością odnotowywania w Rejestrze ww. informacji sprawuje ABI/ASI.

ROZDZIAŁ 9
Procedury wykonywania przeglądów i konserwacji systemu

§ 16

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system/aplikacja.
2. Przeglądy i konserwacja urządzeń
   a) przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej dla danego systemu/aplikacji powinny być wykonywane w terminach określonych przez producenta sprzętu,
   b) jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decydują ASI/ABI,
   c) przegląd i konserwacja urządzeń, może być wykonana na żądanie przełożonego ASI/ABI,
   d) czynności, o których mowa w § 16 ust 2 lit a) i lit b) wykonują ASI/ABI co najmniej jeden raz na kwartał,
   e) nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości ASI/ABI informuje Burmistrza Toszka,

§ 17

1. Przegląd systemów/aplikacji i narzędzi programistycznych przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
   a) zmiany wersji oprogramowania systemu/aplikacji,
   b) zmiany wersji oprogramowania na stanowisku komputerowym użytkownika,
   c) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowany jest system/aplikacja,
   d) zmiany systemu operacyjnego na stanowisku komputerowym użytkownika,
   e) wykonania zmian w systemie/aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu.
2. Przed dokonaniem zmian w systemie/aplikacji należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno m.in. obejmować:
   a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),

b) poprawność działania funkcjonalności systemu/aplikacji sprawdzonej na różnego typu danych,

c) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty, itp.).

3. Za prawidłowość przeprowadzenia procesu przeglądu i konserwacji systemu/aplikacji odpowiada ASI/ABI.

§ 18

Konserwacja systemów/aplikacji wykorzystywanych przez użytkowników.

1. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu/aplikacji potrzeby wprowadzenia zmian pozwalających dostosować funkcjonalność systemu/aplikacji do obsługi bieżących i planowanych potrzeb Urzędu Miejskiego w Toszku. Zgłoszenia kierowane jest do Biura Informatyki.

ROZDZIAŁ 10
Postanowienia końcowe

§ 19

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
2. Rozporządzenie 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).

wz. BURMISTRZA
Maria [illegible]
2-ga Burmistrza

Załącznik nr 2
Do zarządzenia nr 403/2010
Burmistrza Toszka
z dnia 30.11.2010

Instrukcja Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych w Urzędzie Miejskim w Toszku

ROZDZIAŁ 1

Postanowienia ogólne.

§ 1

1. Instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzania zarówno w zbiorach informatycznych, jak i w zbiorach manualnych. Instrukcję stosuje się także w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.
2. Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych, przetwarzanie danych (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie) oraz usuwanie (zmiana lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą).
3. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są:

- pracownicy upoważnieni do przetwarzania danych osobowych,
- kierownicy komórek organizacyjnych,
- administrator bezpieczeństwa informacji - w przypadku naruszenia systemów informatycznych.

ROZDZIAŁ 1

II. Tryb postępowania w sytuacji naruszenia ochrony danych osobowych.

§ 2

Każdy pracownik Urzędu Miejskiego w Toszku, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym, powinien:

a) powstrzymać się od rozpoczęcia lub kontynuowania jakiejkolwiek czynności lub pracy mogącej spowodować zatarcie śladów bądź dowodów naruszenia,
b) podjąć, stosownie do zaistniałej sytuacji, niezbędne działania celem zapobiegania dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych,

c) niezwłocznie powiadomić o zdarzeniu przełożonego, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych administratora bezpieczeństwa informacji Administrator bezpieczeństwa informacji, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1. zarejestrować zgłoszenie w odpowiednim rejestrze odnotowując wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu, dane osoby zgłaszającej, datę i godzinę zgłoszenia oraz jego treść,
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
5. 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.

6. szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
7. 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.

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.

- Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
- Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
- Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji sporządza z przebiegu zdarzenia raport, w którym zamieszcza, w szczególności informacje o :

1. ustaleniach dotyczących sytuacji naruszenia ochrony danych osobowych,
2. przeprowadzonych czynnościach,
3. podjętych decyzjach i ich uzasadnieniu,
4. wnioski i propozycje ewentualnego podniesienia zabezpieczeń w systemie przetwarzania

wz. BURMISTRZA
Maria [illegible] Kowalskiej
Z-ca Burmistrza