Zarządzenie Nr 399

Prezydenta Miasta Piotrkowa Trybunalskiego

z dnia 20 września 2013 roku

w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji w zakresie ochrony danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego" oraz „Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych"

Na podstawie art. 31, art. 33 ust. 1, 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r., poz. 594 z późn. zm.), ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3 ust. 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 informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), **z a r z ą d z a m** co następuje:

§ 1.

Wprowadzam **„Politykę Bezpieczeństwa Informacji w zakresie ochrony danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego"** oraz **„Instrukcję Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych"** stanowiącymi załączniki do niniejszego zarzadzenia.

§ 2.

Celem **„Polityki Bezpieczeństwa Informacji w zakresie ochrony danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego"** jest ustalenie wytycznych bezpieczeństwa danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego.

§ 3.

Celem **„Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych"** jest określenie zasad właściwego zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

§ 4.

W celu realizacji niniejszego zarządzenia zobowiązuję kierowników komórek organizacyjnych oraz wszystkich pracowników Urzędu Miasta Piotrkowa Trybunalskiego do realizacji zapisów zawartych w **„Polityce Bezpieczeństwa Informacji w zakresie ochrony danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego"** oraz **„Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych"** na swoich stanowiskach pracy.

§ 5.

Wykonanie Zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 6.

Nadzór nad wykonaniem Zarządzenia powierzam Sekretarzowi Miasta.

§ 7.

Zarządzenie wchodzi w życie z dniem podpisania.

Z up. PREZYDENTA MIASTA

Andrzej Kacperek

WICEPREZYDENT MIASTA

Załącznik nr 1
Do Zarządzenia Nr..599..
Prezydenta Miasta Piotrkowa Trybunalskiego
z dnia..20.09.2012..

POLITYKA BEZPIECZEŃSTWA INFORMACJI
W ZAKRESIE OCHRONY DANYCH OSOBOWYCH
W URZĘDZIE MIASTA PIOTRKOWA TRYBUNALSKIEGO

I. Kierownictwo Urzędu Miasta Piotrkowa Trybunalskiego świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Urzędowi swoje dane osobowe do właściwej i skutecznej ochrony tych danych zapewnia:

1. Podejmowanie wszystkich działań z zakresu bezpieczeństwa danych osobowych niezbędnych dla ochrony praw osób fizycznych,
2. Stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Urzędzie Miasta Piotrkowa Trybunalskiego w zakresie problematyki bezpieczeństwa tych danych,
3. Podejmowanie w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

II. Kierownictwo Urzędu Miasta świadome jest zagrożeń związanych z przetwarzaniem przez Urząd Miasta danych osobowych, w szczególności z zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych. Urząd Miasta Piotrkowa Trybunalskiego będzie stale doskonalił i rozwijał organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom związanym z:

- infekcjami wirusów i koni trojańskich, które instalując się na komputerze mogą wykradać zasoby tego komputera (zarówno stacjonarne jak i sieciowe),
- wiadomościami poczty elektronicznej typu spam, posiadającymi niekiedy programy pozwalające wykradać zasoby komputera,
- dostępem do stron internetowych, na części których zainstalowane są skrypty pozwalające wykradać zasoby komputera,
- ogólnie dostępnymi komunikatorami internetowymi, w których występują luki, przez które można uzyskać dostęp do komputera,
- związanym z użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku poza Urzędem Miasta,
- możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki,
- możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane,
- lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez zabezpieczenia,
- brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy,
- atakami z sieci uniemożliwiającymi przetwarzanie danych,
- działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
- kradzieżą sprzętu lub nośników z danymi, które zazwyczaj są niezabezpieczone,
- przekazywaniem sprzętu z danymi do serwisu,
- kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
- podszywaniem się przez osoby nieuprawnione pod witrynę internetową, zbierającą dane,
- innym zagrożeniom mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

III. Kierownictwo Urzędu Miasta świadome, jak ważna jest ochrona danych osobowych, wdrożyło i stale utrzymuje Zintegrowany System Zarządzania Jakością i Bezpieczeństwem Informacji zgodny z międzynarodowymi standardami norm ISO, w szczególności zaś spełnia wymagania normy ISO/IEC 27001:2005, co potwierdzone jest certyfikatem przyznanym przez międzynarodową jednostkę certyfikującą. Zgodnie z wymogami tej normy Urząd Miasta jest corocznie audytowany pod kątem utrzymania i rozwijania ochrony przetwarzanych w Urzędzie Miasta informacji, zwłaszcza danych osobowych. Zasady funkcjonowania ochrony informacji i danych osobowych zawarte są w Księdze Jakości i Bezpieczeństwa Informacji, a dla stosowania tych zasad wdrożono 10 polityk bezpieczeństwa informacji:

- Politykę szacowania ryzyka,
- Politykę tworzenia kopii zapasowych i archiwizacji informacji,
- Politykę postępowania ze sprzętem i nośnikami danych,
- Politykę kontroli dostępu do systemu,
- Politykę czystego biurka i czystego pulpitu,
- Politykę zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji,
- Politykę dostępu do pomieszczeń w strefach bezpieczeństwa,
- Politykę kontroli oprogramowania,
- Politykę zarządzania zabezpieczeniami kryptograficznymi,
- Politykę ciągłości działania.

Księga Jakości i Bezpieczeństwa Informacji oraz polityki bezpieczeństwa dostępne są dla pracowników, w sieci wewnętrznej, na stronie www.iso.piotrkow.pl
Ponadto ochrona danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego spełnia standardy kontroli zarządczej.

IV. Na podstawie art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r. Dz. U. Nr 101, poz. 926 z późniejszymi zmianami) oraz § 3 i § 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. z 2004 r. Nr 100, poz. 1024) ustala się następujące wytyczne polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta Piotrkowa Trybunalskiego w związku z realizacją celów strategicznych i operacyjnych Urzędu Miasta.

I. POSTANOWIENIA OGÓLNE

Art. 1

1. Dane osobowe w Urzędzie Miasta przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
   1) przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami) oraz przepisów wykonawczych z nią związanych,
   2) przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących działania publiczne (tekst jednolity Dz. U. z 2013 r., poz 235)
   3) przepisów rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r., poz. 526).
2. Dane osobowe w Urzędzie Miasta przetwarzane są w celu realizacji celów strategicznych i operacyjnych miasta na prawach powiatu.

W szczególności dane osobowe przetwarza się:

1) dla zabezpieczania prawidłowego toku realizacji zadań Urzędu Miasta wynikających z przepisów ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jednolity Dz. U. z 2013 r. poz. 594);
2) w celu zapewnienia prawidłowej, zgodnej z prawem i celami Urzędu Miasta polityki kadrowej;
3) dla realizacji innych, prawnie usprawiedliwionych celów Administratora Danych Osobowych, z poszanowaniem praw i wolności osób powierzających Urzędowi swoje dane.

Art. 2

Definicje.
Ilekroć w niniejszym dokumencie jest mowa o:

1. Urzędzie Miasta – należy przez to rozumieć Urząd Miasta Piotrkowa Trybunalskiego;
2. Administratorze Danych Osobowych (ADO) – należy przez to rozumieć Prezydenta Miasta Piotrkowa Trybunalskiego;
3. Administratorze Bezpieczeństwa Informacji (ADI) – należy przez to rozumieć pracownika Urzędu Miasta wyznaczonego przez ADO do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
4. Administratorze Systemów i Sieci Teleinformatycznych (ASI) – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemów informatycznych Urzędu Miasta oraz stosowanie technicznych i organizacyjnych środków ochrony;
5. Osobie upoważnionej – osoba posiadająca formalne upoważnienie wydane przez ADO lub przez osobę wyznaczoną, uprawnioną do przetwarzania danych osobowych;
6. Użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do bezpośredniego dostępu do danych osobowych w systemie informatycznym, użytkownikiem systemu może być pracownik Urzędu Miasta, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Urzędzie Miasta lub wolontariusz;
7. Przetwarzaniu danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
8. Systemie informatycznym – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9. Zintegrowanym Systemem Zarządzania Jakością i Bezpieczeństwem Informacji – wdrożony, utrzymywany i stosowany system zarządzania zgodny z normami ISO 9001:2008 oraz 27001:2005 zwany dalej ZSZJiBI.

Art. 3

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Miasta odnosi się do danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

Art. 4

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2. Pod szczególną ochroną w Urzędzie Miasta Piotrkowa Trybunalskiego pozostają wrażliwe dane osobowe wymienione w art. 27 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
   Przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym dopuszczalne jest tylko w związku z realizacją celów Urzędu Miasta i w granicach wynikających z przepisów art. 27 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Art. 5

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:
   1) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zabraniem przez osobę nieuprawnioną,
   3) przetwarzaniem z naruszeniem ustawy,
   4) zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dąży do systematycznego polepszania stosowanych informatycznych, technicznych i organizacyjnych środków ochrony tych danych.
3. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego zapewnia aktualizacje informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz inni zagrożeniami danych, płynącymi z funkcjonowania systemu informatycznego oraz sieci telekomunikacyjnych.

Art. 6

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje kontrolę i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów.
2. Niszczenie zbędnych danych osobowych i/lub ich zbiorów polega w szczególności na:
   1) trwałym, fizycznym zniszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane, przy zastosowaniu powszechnie dostępnych metod.
   2) anonimizacji danych osobowych i/lub ich zbiorów polegającej na pozbawieniu danych osobowych i/lub ich zbiorów cech pozwalających na identyfikacje osób fizycznych, których anonimizowane dane dotyczą.
3. Osoby przetwarzające dane osobowe w Urzędzie Miasta mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych osobowych i/lub ich zbiorów.
4. Kontrola i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów polega na sprawdzaniu stosowania procedur niszczenia danych, opisanych w Księdze Jakości Bezpieczeństwa Informacji, w trakcie audytów wewnętrznych i zewnętrznych.

Art. 7

Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki ochrony tych danych. W skład tej dokumentacji wchodzą w szczególności:
1) zarządzenia Prezydenta Miasta odnoszące się do kwestii bezpieczeństwa danych osobowych;
2) Polityka bezpieczeństwa informacji w zakresie ochrony danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego;
3) Instrukcja zarządzania systemami informatycznymi, określająca sposób zarządzania i formy zabezpieczeń służących do przetwarzania danych osobowych w Urzędzie Miasta;

4) Księga Jakości i Bezpieczeństwa Informacji wraz z Politykami bezpieczeństwa, funkcjonujące w ramach Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwem Informacji i określające m. in. środki techniczne i organizacyjne niezbędne dla zapewnienia poufności i integralności danych (rozliczalność przetwarzanych danych zapewnia system nVision);
5) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. Wykaz prowadzony jest w systemie nVision przez ASI;
6) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Wykaz prowadzony jest przez ABI;
7) opisy struktur zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Dokumentacja prowadzona jest przez ASI i zapisana w zasobach sieciowych;
8) opis sposobu przepływu danych pomiędzy poszczególnymi systemami prowadzony jest przez ASI i zapisany w zasobach sieciowych;

II. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Art. 8

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych udostępnia przetwarzane na jego obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy uregulowań wewnętrznych obowiązujących w tym zakresie.
2. Imienne upoważnienie, o którym mowa w ust. 1, zawierające zakres upoważnienia, oświadczenie osoby upoważnionej oraz potwierdzenie przeszkolenia z zasad ochrony danych osobowych, podpisywane jest przez ADO lub osobę przez niego upoważnioną. Upoważnienie wystawiane jest na wniosek przełożonego.
3. ABI prowadzi w pliku elektronicznym:
   - Rejestr Upoważnień wydawanych w danym roku lub Projekcie,
   - ewidencję alfabetyczną upoważnień wydanych pracownikom Urzędu Miasta.

Art. 9

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych.
2. Dysponentami danych osobowych są osoby, które powierzyły swoje dane Urzędowi Miasta w związku z realizacją jego zadań.

Art. 10

1. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonej kategorii, w tym dysponenci danych osobowych, mające interes prawny w uzyskaniu dostępu do tych danych mogą mieć do nich wgląd wyłącznie w obecności upoważnionego pracownika Urzędu Miasta.
2. Zasada wyrażona w ust. 1 ma także zastosowanie do przypadku korzystania przez związki zawodowe z uprawnień przysługujących im na mocy ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity z 1998 r.: Dz. U. Nr 21, poz. 94 z późniejszymi zmianami) i ustawy z dnia 23 maja 1991 r. o związkach zawodowych (tekst jednolity z 2001 r.: Dz. U. Nr 79, poz. 854 z późniejszymi zmianami).

Art. 11

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia administratora danych osobowych lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. W szczególności dostęp do danych osobowych na wskazanej w ust. 1 zasadzie mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, sądy powszechne, Najwyższa Izba Kontroli, Generalny

Inspektor Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień – po okazaniu dokumentów potwierdzających te uprawnienia.

III. OSOBY PRZETWARZAJĄCE DANE OSOBOWE

Art. 12

1. Na podstawie art. 7 ust. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, osobą odpowiedzialną za bieżącą realizację polityki ochrony danych osobowych na terenie Urzędu Miasta Piotrkowa Trybunalskiego jest Prezydent Miasta - ADO.
2. Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ADO wyznacza Administratora Bezpieczeństwa Informacji (ABI) nadzorującego przestrzeganie zasad ochrony danych osobowych.
3. ADO wyznacza, w drodze zarządzenia, Administratora Systemów i Sieci Teleinformatycznych (ASI) odpowiadającego za ochronę fizyczną, elektromagnetyczną i kryptograficzną danych osobowych oraz bezpieczeństwo transmisji w sieciach służących do wytwarzania, przetwarzania, przechowywania informacji zawierających dane osobowe.
4. Pracownicy przetwarzający dane osobowe są odpowiedzialni za przestrzeganie zasad ochrony danych osobowych wynikającym z przepisów prawa oraz uregulowań wewnętrznych na swoim stanowisku pracy.

Art. 13

Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dopuszcza do ich przetwarzania w systemie informatycznym i/lub tradycyjnym wyłącznie osoby posiadające upoważnienie nadane przez ADO.

Art. 14

Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia kontrolę nad dostępem do tych danych. Kontrola ta w szczególności realizowana jest poprzez ewidencjonowanie osób przetwarzających dane osobowe oraz audyty wewnętrzne i zewnętrzne Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwem Informacji sprawdzające, czy wszystkie osoby przetwarzające dane osobowe mają odpowiednie upoważnienia do ich przetwarzania.

Art. 15

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zaznajomienie osób upoważnionych do dostępu i/lub przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Urzędzie Miasta.
2. W szczególności osoby, wskazane w ust. 1, zaznajamiane są z kwestiami wymienionymi w tych przepisach przed dopuszczeniem do pracy na stanowiskach związanych z przetwarzaniem danych osobowych, a także odpowiednio, w trakcie trwania zatrudnienia – w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub technikach i środkach ochrony danych stosowanych w Urzędzie Miasta.
3. Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Urzędzie Miasta może odbywać się w szczególności poprzez:
   1) instruktaż na stanowisku pracy,
   2) wewnętrzny biuletyn informacyjny ISON,
   3) obieg wewnętrzny dokumentów w systemie IntraDOK,
   4) udostępnienie programu LEX Polonica,
   5) szkolenie wewnętrzne realizowane na terenie Urzędu Miasta.

Art. 16

Osoby upoważnione przez ADO do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych ochroną w związku z wykonywaną przez siebie pracą. W szczególności są one informowane o powinności chronienia danych osobowych oraz sposobów ich zabezpieczenia, stosowanych w Urzędzie Miasta.

IV. PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE PRZEZ URZĄD MIASTA PIOTRKOWA TRYBUNALSKIEGO

Art. 17

Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego zapewnia osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jego celów, realizację praw wynikających z zapisów Rozdziału 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami).

V. BUDYNKI, POMIESZCZENIA I CZĘŚCI POMIESZCZEŃ, TWORZĄCE OBSZAR URZĘDU MIASTA, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Art. 18

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza budynki, pomieszczenia i części pomieszczeń, tworzące obszar Urzędu Miasta, w którym przetwarzane są dane osobowe.
2. W przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.
3. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności dokonane poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych uniemożliwiające, lub co najmniej ograniczające, niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.
4. Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego Urzędu Miasta. W szczególności stacje robocze (komputery) wchodzące w skład tego systemu, powinny być umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.
5. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe jest tworzony, przechowywany i aktualizowany jest w systemie nVision przez ASI.
6. W budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar Urzędu Miasta, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu i/lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrole nad bezpieczeństwem przetwarzania tych danych.
7. Osoby nieupoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności niemające związku z dostępem do tych danych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar Urzędu Miasta, w którym przetwarzane są dane osobowe – wyłącznie w obecności upoważnionego pracownika Urzędu Miasta, lub – w razie jego nieobecności – na podstawie upoważnienia wydanego przez ADO lub inną upoważnioną osobę.
8. Szczegółowe zasady postępowania zawarte są w ZSZJiBI, tj:
   - Polityce dostępu do pomieszczeń w strefach bezpieczeństwa,
   - Polityce kontroli dostępu do systemu,
   - Polityce czystego biurka i czystego pulpitu.

Art. 19

1. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
2. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych jest on obowiązany umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych osobom niepowołanym.
3. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku i/lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i może zostać potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
4. Szczegółowe zasady postępowania zawarte są w ZSZJiBI, tj:
   - Polityce dostępu do pomieszczeń w strefach bezpieczeństwa,
   - Polityce kontroli dostępu do systemu,
   - Polityce czystego biurka i czystego pulpitu.

Art. 20

1. Dostęp do budynków i pomieszczeń Urzędu Miasta, w których przetwarzane są dane osobowe podlega kontroli.
2. Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia / budynku oraz godzinę pobrania lub zdania klucza.
3. Klucze do budynków i/lub pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych budynków, lub pomieszczeń na innych zasadach.
4. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
5. Szczegółowe zasady kontroli dostępu do poszczególnych obszarów (budynków, pomieszczeń) Urzędu Miasta określone są w ZSZJiBI, tj:
   - Polityce dostępu do pomieszczeń w strefach bezpieczeństwa.

VI. ZBIORY DANYCH OSOBOWYCH TWORZONE W URZĘDZIE MIASTA PIOTRKOWA TRYBUNALSKIEGO

Art. 21

1. Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych tworzonych na jego obszarze.
2. Wykaz zbiorów danych osobowych jest przechowywany i aktualizowany przez ABI.

Art. 22

Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zgodną z przepisami rozdziału 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ochronę zbiorom danych osobowych sporządzanym doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z innymi zadaniami realizowanymi przez Urząd Miasta, poprzez ich niezwłoczne usuwanie lub poddanie anonimizacji po wykorzystaniu.

Art. 23

Administrator Danych Osobowych Urzędu Miasta Piotrkowa Trybunalskiego realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zabrania tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych, niż niezbędne dla realizacji celów Urzędu Miasta.

Z up. PREZYDENTA MIASTA

Andrzej Kacperek

WICEPREZYDENT MIASTA

Załącznik nr 2
Do Zarządzenia Nr. 599
Prezydenta Miasta Piotrkowa Trybunalskiego
z dnia 20.09.2012

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA PIOTRKOWA TRYBUNALSKIEGO

I . Cel instrukcji

Celem niniejszego dokumentu jest określenie zasad właściwego zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład, urządzenia, odpowiednio do skali zagrożeń i kategorii danych objętych ochroną.
Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez URZĄD MIASTA PIOTRKOWA TRYBUNALSKIEGO w systemach informatycznych rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

II . Podstawa prawna:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.)
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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)

II . Zakres stosowania

Instrukcję stosuje się do danych osobowych przetwarzanych w systemach informatycznych, danych osobowych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.
Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem informatycznym. W przypadku wystąpienia potrzeb wprowadzenia nowych lub modyfikacji istniejących zasad bezpieczeństwa przetwarzania danych osobowych w systemie, wnioski o ich uwzględnienie i wdrożenie powinni składać kierownicy komórek organizacyjnych, w których przetwarzane są dane osobowe, bezpośrednio do Administratora Bezpieczeństwa Informacji.

III . Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1. Urzędzie Miasta – należy przez to rozumieć Urząd Miasta Piotrkowa Trybunalskiego;
2. Administratorze Danych Osobowych (ADO) – należy przez to rozumieć Prezydenta Miasta Piotrkowa Trybunalskiego;

3. Administratorze Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć pracownika Urzędu Miasta wyznaczonego przez ADO do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
4. Administratorze Systemów i Sieci Teleinformatycznych (ASI) – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemów informatycznych Urzędu Miasta oraz stosowanie technicznych i organizacyjnych środków ochrony;
5. Osobie upoważnionej – należy przez to rozumieć osobę posiadającą formalne upoważnienie wydane przez ADO lub przez osobę wyznaczoną, uprawnioną do przetwarzania danych osobowych;
6. Użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do bezpośredniego dostępu do danych osobowych w systemie informatycznym, użytkownikiem systemu może być pracownik Urzędu Miasta, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Urzędzie Miasta lub wolontariusz;
7. Przetwarzaniu danych osobowych – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
8. Systemie informatycznym – należy przez to rozumieć zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9. Zintegrowanym Systemem Zarządzania Jakością i Bezpieczeństwem Informacji – należy przez to rozumieć wdrożony, utrzymywany i stosowany system zarządzania zgodny z normami ISO 9001:2008 oraz 27001:2005 zwany dalej ZSZJiBI;
10. Sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu Miasta wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci Telekomunikacyjnych;
11. Sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

IV. Zarządzanie bezpieczeństwem systemów

1. Podstawowe cele zabezpieczeń danych
   1.1. Podstawowym celem zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa tych danych, które są w nich przetwarzane.
   1.2. W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu informatycznego przetwarzającego dane osobowe powinien być możliwy wyłącznie po podaniu identyfikatora odrębnego dla każdego użytkownika systemu i poufnego hasła lub innego elementu uwierzytelniającego.
2. Podstawowe zasady zabezpieczeń systemów
   1.1. Należy zapewnić poufność, integralność i rozliczalność systemów informatycznych służących do przetwarzania danych osobowych.
   1.2. Należy zapewnić aby użytkownicy systemów informatycznych służących do przetwarzania danych osobowych nie posiadali wyższych poziomów uprawnień w tych systemach niż wymagane do wykonywania powierzonych obowiązków (dostępność).
   1.3. Należy zapewnić aby wszelkie działania użytkowników systemów informatycznych zapewniały rozliczalność tych działań.
2. Prawidłowy poziom zabezpieczeń danych
   2.1. Prawidłowy poziom zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych zostaje zapewniony poprzez przestrzeganie następujących zasad:
   - uniemożliwienie osobom postronnym uzyskiwania nieupoważnionego dostępu do systemu;
   - instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania wyłącznie przez uprawnionych użytkowników systemu;
   - niepodejmowanie przez użytkowników systemu prób testowania, modyfikacji i naruszenia zabezpieczeń systemu lub jakichkolwiek działań noszących takie znamiona.

V . Procedury nadawania i zmiany uprawnień do przetwarzania danych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych ma obowiązek zapoznać się z:
   1.1. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.);
   1.2. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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),
   1.3. Polityką Bezpieczeństwa Informacji oraz dokumentacją Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwem Informacji w Urzędzie Miasta Piotrkowa Trybunalskiego opublikowanych na stronie www.iso.piotrkow.pl;
   1.4. niniejszą instrukcją.
2. Zapoznanie się z przepisami wymienionymi w punkcie 1 pracownik potwierdza własnoręcznym podpisem na KARCIE POTWIERDZENIA ZAPOZNANIA PRACOWNIKA Z DOKUMENTAMI W ZWIĄZKU Z ZATRUDNIENIEM.
3. Administratorzy przyznają uprawnienia w zakresie dostępu do systemów informatycznych na podstawie wniosku bezpośredniego przełożonego pracownika określającego zakres uprawnień pracownika zgodnie z polityką SZBI Pol_04 Polityka kontroli dostępu do systemu.
4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
5. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
6. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
7. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych.
8. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy.
9. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
10. Kierownicy komórek organizacyjnych zobowiązani są informować Kierownika Referatu Informatyki o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
11. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

VI . Zasady posługiwania się hasłami

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i hasła.
2. Hasło powinno być zmieniane przez użytkownika, co najmniej raz w miesiącu. W przypadku gdy funkcjonalność danego systemu nie zapewnia automatycznego wymuszania zmiany haseł, należy zobligować pracowników do samodzielnej zmiany haseł, zgodnie z zasadami przyjętymi dla danego systemu informatycznego.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Przy wyborze hasła obowiązują następujące zasady:
   8.1. minimalna długość hasła - 8 znaków;
   8.2. zakazuje się stosować:
      8.2.1. swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
      8.2.2. swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
      8.2.3. imion (w szczególności imion osób z najbliższej rodziny),
      8.2.4. ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp.,
      8.2.5. wyrazów słownikowych,
      8.2.6. przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.,
      8.2.7. identyfikatora użytkownika;
   8.3. należy stosować:
      8.3.1. hasła zawierające kombinacje liter i cyfr,
      8.3.2. hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp., o ile system informatyczny na to pozwala,
      8.3.3. hasła, które można zapamiętać bez zapisywania,
      8.3.4. hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.
9. Zmiany hasła nie wolno zlecać innym osobom.
10. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
11. Użytkownicy powinni być świadomi swojej odpowiedzialności za utrzymanie skutecznej kontroli dostępu, szczególnie w odniesieniu do haseł i zabezpieczenia swojego sprzętu.
12. Hasło użytkownika o prawach administratora powinno znajdować się w zamykanej na klucz szafie metalowej, do której dostęp ma ASI.

VII . Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
6. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie swojego przełożonego lub kierownika referatu informatyki bądź ABI.

VIII . Procedury tworzenia zabezpieczeń

1. Za systematyczne przygotowanie kopii bezpieczeństwa (dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia) odpowiada kierownik referatu informatyki (ASI).

2. Kopie bezpieczeństwa wykonywane są zgodnie z polityką SZBI Pol_02 Polityka tworzenia kopii zapasowych i archiwizacji informacji, i przechowywane w dwóch różnych lokalizacjach.
3. Płyty CD-R/DVD-R przechowuje się w kasie pancernej w pokoju 105 w budynku Urzędu Miasta, Pasaż Karola Rudowskiego 10.
4. W przyjętym systemie archiwizacji za ochronę danych na dyskach lokalnych odpowiedzialny jest użytkownik na danym stanowisku pracy.

IX . Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruki

1. Elektroniczne nośniki informacji:
   1.1. Generalnie nie przewiduje się tworzenia nośników elektronicznych zawierających dane osobowe poza sytuacjami wystąpienia wyższej konieczności utworzenia takiego nośnika;
   1.2. Sposób postępowania z nośnikami elektronicznymi zawierającymi dane osobowe określony jest w Pol_03 Polityka postępowania ze sprzętem i nośnikami danych ZSZJiBI;
   1.3. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określonych w ZSZJiBI;
   1.4. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach;
   1.5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   1.6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
2. Kopie zapasowe:
   2.1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w kasie pancernej w pokoju 105 w budynku Urzędu Miasta Pasaż Karola Rudowskiego 10;
   2.2. Dostęp do danych opisanych w punkcie 2.1 ma kierownik referatu informatyki, ASI, ABI oraz upoważnieni pracownicy referatu informatyki.
3. Wydruki:
   3.1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym;
   3.2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy;
   3.3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

X . Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Definicje wzorców wirusów powinny być aktualizowane przynajmniej raz w czasie dnia.
3. Zasady opisane są w polityce Pol_08 Polityka kontroli oprogramowania ZSZJiBI.
4. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
5. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
6. W przypadku wystąpienia alertów wirusowych (wykrycia wirusów komputerowych) postępuje się zgodnie z polityką Pol_06 Polityka zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji ZSZJiBI.

XI . Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani pocztą elektroniczną.
3. Udostępnienie danych osobowych następuje po przedstawieniu wniosku wg wzoru określonego w procedurach referatu ewidencji ludności i opublikowanych na stronie www.bom.piotrkow.pl.
4. Pracownicy prowadzą rejestry udostępnionych danych osobowych zawierające, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.
5. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

XII . Postępowanie w sytuacji naruszenia ochrony danych osobowych

Postępowanie w sytuacji naruszenia ochrony danych osobowych określa poniższa procedura:

Procedura regulująca postępowanie pracowników Urzędu Miasta Piotrkowa Trybunalskiego zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych.

1. Celem niniejszej procedury jest określenie zadań i sposób postępowania pracowników zatrudnionych przy przetwarzaniu danych osobowych aby móc prawidłowo wykrywać i właściwie reagować na przypadki naruszenia ochrony danych osobowych.
2. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:
   1.1. stanu urządzeń technicznych;
   1.2. zawartości zbiorów danych osobowych;
   1.3. sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej;
   1.4. metod pracy (w tym obiegu dokumentów).

3. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:
   3.1. powiadomić bezpośredniego przełożonego lub kierownika referatu informatyki lub ABI bądź ADO.
   3.2. zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych;
   3.3. podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia - o ile czynności te nie spowodują przekroczenia uprawnień pracownika;
   3.4. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.
4. Bezpośredni przełożony pracownika po otrzymaniu powiadomienia o naruszenia bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić ABI lub ADO chyba, że zrobił to uprzednio pracownik, który stwierdził naruszenie.
5. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych, ABI i osoba przełożona pracownika przejmują nadzór nad pracą w systemie odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.
6. ABI lub osoba przez niego wyznaczona podejmuje czynności wyjaśniające mające na celu ustalenie:
   6.1. przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych;
   6.2. osób winnych naruszenia bezpieczeństwa danych osobowych;
   6.3. skutków naruszenia.

7. ABI zobowiązany jest do powiadomienia o zaistniałej sytuacji ADO, który podejmuje decyzję o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.
8. ABI zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego, co najmniej:
   8.1. datę i miejsce wystąpienia naruszenia;
   8.2. zakres ujawnionych danych;
   8.3. przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy;
   8.4. sposób rozwiązania problemu;
   8.5. przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
9. Raport ten ABI przekazuje ADO.
10. W przypadku następującego permanentnie naruszenia ochrony danych osobowych bezwzględnie należy:
    10.1. zawiadomić Generalnego Inspektora Danych Osobowych o zaistniałym przypadku,
    10.2. zabezpieczyć kopie archiwalne danych,
    10.3. cofnąć uprawnienia wszystkich użytkowników posiadających dostęp do zagrożonej bazy danych osobowych.

XIII . Procedury wykonywania przeglądów i konserwacji systemu

1. Przeglądy i konserwacja urządzeń:
   1.1. Zasady postępowania opisane są w polityce Pol_03 Polityka postępowania ze sprzętem i nośnikami danych ZSZJiBI.
2. Przegląd programów i narzędzi programowych:
   2.1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów;
   2.2. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji jest trwale zapisane w bazie danych programu. Ponadto w Urzędzie Miasta wykorzystywany jest system monitorowania umożliwiający rozliczalność każdego użytkownika.
3. Rejestracja działań konserwacyjnych, awarii oraz napraw:
   Zasady postepowania opisane są w polityce Pol_03 Polityka postępowania ze sprzętem i nośnikami danych ZSZJiBI oraz w polityce Pol_06 Polityka zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji ZSZJiBI.

XIV. Zarządzanie bezpieczeństwem sieci

1. Kierownik referatu informatyki powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez:
   - kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
   - kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
2. Wewnętrzna adresacja IP, konfiguracja oraz informacja o systemach powiązanych nie powinna być ujawniana osobom nieuprawnionym bez akceptacji ze strony uprawnionej do tego celu osoby.
3. Podłączanie do infrastruktury sieciowej nieautoryzowanych urządzeń takich jak modemy, urządzenia sieciowe, w tym urządzenia sieci bezprzewodowych jest zabronione.
4. Podłączanie we własnym zakresie stacji roboczych do publicznej sieci telekomunikacyjnej poprzez nieautoryzowane urządzenia sieciowe, będąc jednocześnie podłączonym do infrastruktury lokalnej LAN jest zabronione.
5. Użytkownikom należy zapewnić dostęp tylko do tych usług infrastruktury teleinformatycznej (np. dostęp do Internetu, zdalny dostęp, poczta elektroniczna) do których zostali autoryzowani.
6. Osoby niebędące pracownikami nie powinny posiadać nieautoryzowanego i niekontrolowanego dostępu do infrastruktury teleinformatycznej.

7. Niezabezpieczone usługi infrastruktury teleinformatycznej, pozwalające przesyłać hasła w postaci niezabezpieczonej (np. telnet lub ftp) nie powinny być wykorzystywane i powinny być zablokowane.
8. Wykonywane połączenia do Internetu są być monitorowane i rejestrowane.
9. Systemy monitorowania połączeń do Internetu powinny rejestrować źródłowy adres IP, datę i godzinę połączenia, wykorzystywany protokół, docelową witrynę lub urządzenie (adres IP) oraz nazwę użytkownika nawiązującego połączenie.
10. Dostęp do Internetu powinien być zabezpieczony poprzez zastosowanie narzędzi służących do blokowania stron internetowych lub usług zawierających niepożądane treści lub zawartość (np. materiały o charakterze pornograficznym, nielegalnym, obraźliwym, szkodliwe oprogramowanie oraz usługi udostępniania plików).
11. Wszystkie pliki ściągnięte z Internetu powinny być sprawdzane przez system antywirusowy.
12. Użytkownicy powinni być uświadamiani o zagrożeniach występujących podczas korzystania z Internetu.
13. Użytkownicy nie powinny instalować żadnego oprogramowania ściągniętego z Internetu bez upewniania się czy został on ściągnięty z zaufanej strony oraz czy nie zagraża bezpieczeństwu systemów informatycznych.
14. Poczta elektroniczna nie może być wykorzystywana do przesyłania informacji zawierających treści obraźliwe, szkodliwe, nielegalne, pornograficzne, dotyczących przekonań politycznych i uprzedzeń rasowych.
15. Wykorzystywanie prywatnych skrzynek pocztowych znajdujących się poza domeną pocztową piotrkow.pl do przesyłania informacji służbowych jest niedozwolone chyba, że zastosowano właściwe zabezpieczenia uzgodnione wcześniej z ABI i ASI.
16. Przychodzące i wychodzące wiadomości poczty elektronicznej należy sprawdzać na wypadek występowania wirusów i kodów złośliwych a potencjalne niebezpieczne załączniki należy blokować.
17. Wiadomości poczty elektronicznej otrzymane z nieznanych i podejrzanych źródeł nie powinny być otwierane i przekazywane dalej.
18. Wewnętrzne adresy poczty elektronicznej nie powinny być udostępniane i ujawniane osobom nieuprawnionym.
19. Wewnętrzna lista adresowa powinna być zabezpieczona przed nieautoryzowanym dostępem i modyfikacją.

XV. Postanowienia końcowe

1. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tj. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
2. Użytkownicy systemu przy przetwarzaniu danych osobowych zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Instrukcji.

Z up. PREZYDENTA MIASTA
Andrzej Kacperek
WICEPREZYDENT MIASTA