Załącznik nr 1 do Zarządzenia nr 26/2009
Burmistrza Miasta I Gminy Ostrzeszów
z dnia 31.03.2009

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

w

Urzędzie Miasta i Gminy w Ostrzeszowie

Ostrzeszów, 2009 r.

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE 3

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI 4

III. ZAKRES 5

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI 7

V. DOSTĘP DO INFORMACJI 8

VI. ZARZĄDZANIE DANYMI OSOBOWYMI 9

VII. ZAKRESY ODPOWIEDZIALNOŚCI 11

VIII. PRZETWARZANIE DANYCH OSOBOWYCH 14

IX. ARCHIWIZOWANIE INFORMACJI ZAWIERAJACYCH DANE OSOBOWE 15

I. POSTANOWIENIA OGÓLNE

§1.

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Urzędzie Miasta i Gminy w Ostrzeszowie grupy informacji zawierającej dane osobowe.

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. Urząd – Urząd Miasta i Gminy w Ostrzeszowie
2. komórka organizacyjna – odpowiednio komórki organizacyjne, dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. przetwarzanie danych osobowych – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. użytkownik – osoba upoważniona do przetwarzania danych osobowych,
5. administrator systemu – osoba upoważniona do zarządzania systemem informatycznym,
6. system informatyczny – system przetwarzania danych w Urzędzie Miasta i Gminy w Ostrzeszowie wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
7. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez Urząd informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
   3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

§4.

1. W systemie informacyjnym Urzędu przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

§5.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Urzędu w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
   2) informacji będących własnością Urzędu lub klientów Urzędu, o ile zostały przekazane na podstawie umów,
   3) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§6.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§7.

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:
   1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
   2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Urzędzie
   3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia.

V. DOSTĘP DO INFORMACJI

§8.

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Urzędzie zasad ochrony danych osobowych.

§9.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§10.

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§11.

Administratorem danych osobowych Burmistrz Miasta i Gminy Ostrzeszów.

§12.

1. Za bezpieczeństwo danych osobowych Urzędu, odpowiadają:
   1) Administrator danych osobowych – Burmistrz Miasta i Gminy Ostrzeszów,
   2) Administrator Bezpieczeństwa Informacji Urzędu.

2. Administrator Bezpieczeństwa Informacji Urzędu realizując politykę bezpieczeństwa informacji ma prawo wydawać instrukcje regulujące kwestie związane z ochroną danych w strukturach Urzędu.

3. W umowach zawieranych przez Urząd winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez Urząd.

§13.

1. Obowiązki wynikające z ustawy o ochronie danych osobowych Burmistrz Miasta i Gminy Ostrzeszów powierza lokalnym administratorom danych- naczelnikom wydziałów - w zakresie podległych im pracowników.

2. Naczelnicy komórek organizacyjnych Urzędu odpowiadają za realizację wymagań obowiązujących przepisów prawa, dotyczących ochrony danych osobowych, z obowiązkiem współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie swoich właściwości.

3. Naczelnicy komórek organizacyjnych Urzędu zobowiązani są do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), Polityką Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemami

informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

4. Zapoznanie się z dokumentami określonymi w ust. 3 pracownicy Urzędu potwierdzają podpisem na „Indywidualnym zakresie czynności osoby zatrudnionej przy przetwarzaniu danych osobowych" (wzór w załączniku nr 5 do Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w Urzędzie i przekazują Administratorowi Bezpieczeństwa Informacji.

§14.

Ochrona zasobów danych osobowych Urzędu jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Urzędu.

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§15.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Urzędu.

§16.

Administrator bezpieczeństwa informacji w Urzędzie Miasta i Gminy Ostrzeszów:

1. odpowiada za realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,
2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3. określa strategię zabezpieczania systemów informatycznych Urzędu,
4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych urzędu,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, w których przetwarzane są dane osobowe,
9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
12. zatwierdza wniosek naczelnika wydziału o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,

13. powiadamia administratora systemu o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
17. prowadzi rejestr zbiorów danych osobowych Urzędu.

§17.

Lokalni administratorzy danych osobowych zobowiązani są do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
2. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
3. wykonywania zaleceń Administratora Bezpieczeństwa Informacji Urzędu w zakresie ochrony danych osobowych,
4. przekazywanie na bieżąco do Administratora Bezpieczeństwa Informacji zaktualizowanych załączników nr 1, 2, 3, 4 do niniejszego zarządzenia,
5. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,
6. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
7. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
8. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
9. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
10. określanie, które osoby i na jakich prawach mają dostęp do danych informacji,
11. przygotowanie zgłoszeń rejestracji Zbiorów Danych do Generalnego Inspektoratu Danych Osobowych, jeżeli mają one charakter danych osobowych i przekazanie do Administratora Bezpieczeństwa Informacji.

Praca Lokalnych Administratorów Danych Osobowych jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

§18.

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5. konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie na wniosek Lokalnego Administratora Danych, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie,
11. wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

Praca Administratora Systemu Informatycznego jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§19.

Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

§20.

Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.

§21.

Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

IX. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§22.

Zasady archiwizacji i brakowania dokumentów reguluje Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikacji i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. Nr 167, poz. 1375).

BURMISTRZ
w.z.
mgr inż. Mariusz Witek
Zastępca Burmistrza