ZARZĄDZENIE NR 205/2008

BURMISTRZA OPOCZNA

z dnia 12.12 2008 r.

w sprawie wdrożenia Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 ze zm.), oraz § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

zarządza się co następuje:

§ 1. Wprowadza się do stosowania *„Dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie"* zwaną dalej ***Polityką Bezpieczeństwa*** w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuję wszystkich pracowników do przestrzegania ***Polityki Bezpieczeństwa*** w Urzędzie Miejskim w Opocznie.

§ 3. Administratorem Bezpieczeństwa Informacji (ABI) wykonującym czynności określone w Zarządzeniu Burmistrza Miasta Opoczno nr 4/2001 z dnia 19 listopada 2001r , jak również w niniejszej dokumentacji jest Pan Dariusz Badura.

§ 4. Wykonanie zarządzenia powierza się Sekretarzowi Miasta.

§ 5. Traci moc Zarządzenie nr 1/2002 Burmistrza Miasta Opoczno z dnia 05 lutego 2002r.

§ 6. Zarządzenie wchodzi w życie z dniem 01.01.2009r.

BURMISTRZ OPOCZNA

Jan Wieruszewski

Załącznik do Zarządzenia Burmistrza Opoczna nr 205 z dnia 12.12.2008 w sprawie wdrożenia Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie

Z A T W I E R D Z A M

Burmistrz Opoczna

/-/ Jan Wieruszewski

Opracował: Administrator Bezpieczeństwa Informacji inż. Dariusz Badura

UM Opoczno Grudzień 2008

Spis Treści:

I. Postanowienia ogólne

1. Zasady przetwarzania danych osobowych zostały opracowane celem wykonania obowiązków określonych w:
   a) art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 ze zm.),
   b) rozporządzeniu 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).

2. Na Dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie zwaną dalej „dokumentacją" składają się następujące dokumenty:
   1) Polityka Bezpieczeństwa Informacji – załącznik nr 1 do dokumentacji,
   2) Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych – załącznik nr 2 do dokumentacji,
   3) Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych – załącznik nr 3 do dokumentacji
   4) Regulamin Sieci Komputerowej – załącznik nr 4 do dokumentacji
   5) Wzór oświadczenia osób upoważnionych do przetwarzania danych osobowych – załącznik nr 5 do dokumentacji
   6) Wzór upoważnienia do przetwarzania danych osobowych – załącznik nr 6 do dokumentacji.
   7) Wzór wniosku o udostępnienie danych osobowych – załącznik nr 7 do dokumentacji

3. Dokumentacja składa się z 47 stron kolejno ponumerowanych.

II. Założenia Bezpieczeństwa Systemów

1. Mając świadomość znaczenia informacji i systemów informacyjnych dla realizacji misji i celów Urzędu Miejskiego w Opocznie zapewniamy, że podejmowane przez Urząd działania dążą do zapewnienia bezpieczeństwa zasobów informacyjnych.
2. W celu udokumentowania Systemu Zarządzania Bezpieczeństwem Informacji przyjmuje się w Urzędzie Miejskim w Opocznie **Dokumentację Systemu Zarządzania Bezpieczeństwem Informacji**.
3. Zasady, Instrukcje działania, kompetencje i zakresy odpowiedzialności opisane w w/w dokumencie obowiązują wszystkich pracowników Urzędu Miejskiego oraz podmioty zewnętrzne współpracujące z Urzędem na mocy umów o przekazaniu danych osobowych.
4. Wdrażany System Zarządzania Bezpieczeństwem Informacji zgodny jest z wymaganiami normy PN-I 07799-2 i będzie nieustannie doskonalony.

III. Cele i strategie bezpieczeństwa Urzędu

1. Cele Urzędu Miejskiego w Opocznie w dziedzinie bezpieczeństwa informacji:
   a. ochrona zasobów informacyjnych Urzędu Miejskiego (UM) i zapewnienie ciągłości działania procesów Urzędu,
   b. ochrona wizerunku Urzędu i wizerunku interesantów,
   c. zapewnienie zgodności z prawem podejmowanych działań,
   d. uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów UM rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
   e. wyznaczenie ogólnych kierunków rozwoju systemu informacyjnego,
   f. podnoszenie kultury informatycznej i tworzenie bezpiecznego społeczeństwa informacyjnego.

2. Cele osiągane są przez realizowane strategie:
   a. zapewnienie wsparcia Zarządzających dla Systemu Bezpieczeństwa Informacji,
   b. właściwa organizacja Systemu Zarządzania Bezpieczeństwem Informacji,
   c. zarządzanie ryzykiem w celu ograniczania go do akceptowanego poziomu,
   d. właściwa ochrona informacji, a w szczególności informacji prawnie chronionych,
   e. zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności systemów informatycznych,
   f. właściwa ochrona informacji związanych z zawartymi umowami,
   g. wdrażanie i rozwój systemów informacyjnych z zachowaniem zasad bezpieczeństwa,
   h. eksploatowanie systemów informacyjnych zgodnie z zasadami bezpieczeństwa,
   i. stała edukacja użytkowników systemu informacyjnego.

IV. Informacje przetwarzane przez system informacyjny Urzędu Miejskiego

1. W systemie informacyjnym Urzędu przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej i rozwoju instytucjonalnego.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.
3. Przetwarzane w Urzędzie informacje są miedzy innymi informacjami dotyczącymi :
   a. informacji publicznych,
   b. danych osobowych,
   c. informacji stanowiących tajemnice Urzędu,
   d. innych informacji prawnie chronionych.
4. Informacje niejawne nie są objęte zakresem niniejszej Polityki.
5. W celu skutecznego zarządzania bezpieczeństwem przetwarzanych informacji zasoby informacyjne są podzielone na grupy informacji.

a. dla każdej grupy zidentyfikowane są zasoby uczestniczące w przetwarzaniu danej informacji,
b. dla każdej grupy zidentyfikowane są wymagania bezpieczeństwa, oszacowane jest ryzyko i na tej podstawie dobrane są odpowiednie zabezpieczenia.

V. Sposób prowadzenie dokumentacji

Dokumentacja przetwarzania danych osobowych prowadzona jest w formie pisemnej. Dokumentacja jest wdrażana do stosowania na podstawie Zarządzenia Burmistrza Opoczna. Wprowadzanie zmian w dokumentacji następuje w tej samej formie.

Załącznik. Nr 1
Do Dokumentacji Systemu Zarządzania
Bezpieczeństwem Informacji
w Urzędzie Miejskim w Opocznie

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Opracował: Administrator Bezpieczeństwa Informacji inż. Dariusz Badura

UM Opoczno Listopad 2008

I. Przepisy ogólne, definicje i objaśnienia

§ 1

1. Polityka Bezpieczeństwa Informacji Urzędu Miejskiego w Opocznie jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach administrowanych przez Urząd Miejski w Opocznie.
2. Przetwarzanie danych osobowych jest dopuszczalne tylko pod warunkiem przestrzegania Ustawy o ochronie danych osobowych z dnia 29 czerwca 1997r (Dz.U.Nr 133, poz.883) i wydanych na jej podstawie przepisów wykonawczych oraz Zarządzenia Burmistrza Opoczna z dnia…… nr …… a także przepisów wdrożonych w Instrukcjach stanowiących załączniki do Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie.

§ 2

1. Podstawowe definicje użyte w niniejszym dokumencie oznaczają:
   a) **Urząd** - Urząd Miejski w Opocznie,
   b) **Wydział / komórka organizacyjna**– odpowiednio wydziały komórki organizacyjne, o których mowa w § 5 „Regulaminu organizacyjnego Urzędu Miejskiego w Opocznie" stanowiącego Załącznik Nr 1 do Zarządzenia Burmistrza Opoczna,
   c) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
   d) **przetwarzanie danych osobowych** – to wszelkie operacje wykonywane na danych osobowych w tym gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
   e) **użytkownik** – osoba upoważniona do przetwarzania danych osobowych,
   f) **identyfikator użytkownika** – ciąg znaków literowych, cyfrowych identyfikujących osobę upoważnioną do przetwarzania danych osobowych,
   g) **hasło** – ciąg znaków znanych wyłącznie użytkownikowi, pozwalający na zalogowanie się do konta użytkownika
   h) **odbiorca danych** – każdy , komu udostępnia się dane osobowe,
   i) **system informatyczny** – system przetwarzania danych to zespół urządzeń, programów, procedur i narzędzi wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje w celu przetwarzania danych.
   j) **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.
   k) **Usuwanie danych** – to trwałe zniszczenie danych uniemożliwiające ich ponowną identyfikację,
   l) **Administrator Bezpieczeństwa Informacji** – ABI
   m) **Administrator Systemu Informatycznego** – ASI

2. 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.

   Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:

   a. **Poufność informacji** - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,

   b. **Integralność informacji** - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,

   c. **Dostępność informacji** - rozumiana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

   d. **Zarządzanie ryzykiem** – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

   e. **Niezaprzeczalności odbioru** - rozumianej jako zdolność systemu Urzędu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,

   f. **Niezaprzeczalności nadania** - rozumianej jako zdolność systemu Urzędu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie.

   g. **Rozliczalności działań** – rozumianej jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.

§ 3

W Urzędzie Miejskim w Opocznie wyznaczono następujące osoby odpowiedzialne za opracowywanie dokumentacji i monitorowanie przestrzegania zasad w niej określonych:

1) Pana Dariusza Badurę - (Administratora Bezpieczeństwa Informacji) za opracowanie Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie , nadzorowanie przestrzegania zasad i procedur określonych w dokumentacji, przechowywanie dokumentacji przetwarzania danych a także przywracanie do stanu prawidłowego w zakresie przyznanych kompetencji i uprawnień oraz przedstawiania raportów w tym zakresie Burmistrzowi,
2) Pana Kazimierza Kożuchowskiego – Sekretarz Miasta za nadzorowanie opracowywania dokumentacji oraz zmian w dokumentacji, a także przedstawienie dokumentacji (zmian) Burmistrzowi do zatwierdzenia,
3) Naczelnicy Wydziałów zobowiązani są do współpracy z ABI celem opracowania w/w dokumentacji oraz zmian w dokumentacji w zakresie odpowiednim do kompetencji i wykonywanych zadań.

.

§ 4

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mogą mieć tylko osoby mające odpowiednie upoważnienie i wpisane do ewidencji prowadzonej przez ABI.
2. Użytkownicy zaangażowani w procesie przetwarzania danych osobowych są zobowiązani do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przechowywania.
3. Użytkownicy są zobowiązani do postępowania zgodnie z Instrukcją określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Opocznie stanowiącą załącznik nr 2 do dokumentacji.
4. Osoby przetwarzające dane są zobowiązane powiadomić ABI o ewentualnych incydentach i naruszeniach bezpieczeństwa systemu ochrony danych we wszystkich zbiorach. Tryb postępowania w w/w sytuacji określa Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych stanowiąca załącznik nr 3 do dokumentacji.

§ 5

W Urzędzie Miejskim zabrania się przetwarzania danych osobowych ujawniających:

a) Pochodzenie rasowe lub etniczne,
b) Poglądy polityczne,
c) Przekonania religijne lub filozoficzne
d) Przynależność wyznaniową,
e) Przynależność partyjną lub związkową,
f) Stan zdrowia, kod genetyczny, nałogi lub fakty z życia seksualnego, chyba że pozwalają na to obowiązujące przepisy prawa lub osoba której powyższe dane dotyczą wyrazi na to pisemną zgodę.

§ 6

Pracownik Urzędu Miejskiego w Opocznie, który:

a) Przetwarza w zbiorze danych dane do których nie jest upoważniony,
b) Przetwarza dane których przetwarzanie jest zabronione,
c) Przetwarza dane niezgodnie z celem stworzenia zbioru danych,
d) Udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
e) Nie zgłasza ABI zbiorów danych podlegających rejestracji,
f) Nie dopełnia obowiązku poinformowania osoby, której dane dotyczą o przysługującej jej prawach,
g) Uniemożliwia osobie, której dane dotyczą korzystanie z przysługujących jej praw,

podlega odpowiedzialności karnej zgodnie z Ustawą z dnia 29 sierpnia 1997 o ochronie danych osobowych z dnia oraz przepisami Kodeksu Pracy.

II. Gromadzenie danych osobowych

§ 7

Dane gromadzone w Urzędzie Miejskim w Opocznie mogą być uzyskiwane:

a) Bezpośrednio od osób których dane dotyczą
b) Z innych źródeł, w granicach dozwolonych przepisami prawa

§ 8

Zbierane dane osobowe muszą byś wykorzystane tylko do celów, w jakich są lub będą przetwarzane. Po wykorzystaniu danych osobowych, powinny być one przechowywane w postaci uniemożliwiającej identyfikację osób których dotyczą.

III. Obowiązek Informacyjny

§ 9

1. Naczelnicy Wydziałów i Komórek Organizacyjnych Urzędu Miejskiego w Opocznie zbierających i przetwarzających dane osobowe są odpowiedzialni za poinformowanie osób, których dane dotyczą o :
   a) Adresie, siedzibie gdzie dane są zbierane i przetwarzane
   b) Celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
   c) Prawie do treści swoich danych oraz możliwości ich poprawiania
2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, należy powiadomić osobę której dane dotyczą o źródle danych oraz uprawnieniach wynikających z art.32 ust.1 pkt 7 i 8 ustawy o ochronie danych

IV. Udzielanie informacji o przetwarzaniu danych osobowych

§ 10

1. Osobom, których dane przetwarza się w zbiorach danych w Urzędzie Miejskim w Opocznie przysługuje prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskiwania wyczerpujących informacji na temat tych danych
2. Każda osoba która wystąpi z wnioskiem o otrzymanie informacji do Urzędu otrzyma odpowiedź na piśmie w terminie nie przekraczającym 30 dni.
3. Wniosek o udostępnienie danych ze zbioru danych osobowych stanowi załącznik nr 7 do niniejszej dokumentacji. Wniosek jest również do pobrania na stronie podmiotowej www.bip.opoczno.pl
4. W przypadku gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Ustawy , albo są zbędne do realizacji celu, dla którego zostały zebrane, ABI jest zobowiązany do ich uzupełnienia, uaktualnienia ,sprostowania lub usunięcia.

V. Rejestracja zbiorów danych osobowych

§ 11

1. Rejestracją zbiorów danych osobowych w GIODO zajmuje się ABI,
2. Naczelnicy Wydziałów i Komórek organizacyjnych Urzędu, w których są przetwarzane dane osobowe zobowiązani są do zgłaszania ABI:
   a) Rejestracji zbiorów danych osobowych przetwarzanych w kierowanych przez nich wydziałach/komórkach,
   b) Planowanego rejestrowania nowych zbiorów danych osobowych,
   c) Wnoszenia zmian zbiorów już zarejestrowanych.

VI. Ochrona przetwarzania danych osobowych

§ 12

1. Wszyscy pracownicy Urzędu Miejskiego w Opocznie zobowiązani są do stosowania środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, a w szczególności przed ich udostępnianiem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.
2. Całkowity nadzór i kontrolę nad przetwarzaniem danych w Urzędzie Miejskim w Opocznie realizuje Administrator Bezpieczeństwa Informacji (ABI) osobiście.
3. ADO wydaje indywidualne upoważnienia osobom przetwarzającym dane osobowe
4. ABI przechowuje wydane przez ADO upoważnienia.
5. ABI prowadzi wykaz osób którym wydano imienne upoważnienie
6. ABI prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych oraz ewidencję zaświadczeń o zachowaniu tajemnicy przy przetwarzaniu danych.
7. ABI zapewnia zapoznanie się i przeszkolenie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych w Urzędzie Miejskim w Opocznie.
8. ABI okresowo będzie analizował zagrożenia i ryzyko w celu weryfikacji środków zabezpieczających, a także dokonywał inwentaryzacji systemów informatycznych i zbiorów danych w celu zapewnienia aktualności procedur i instrukcji przy przetwarzaniu danych osobowych.
9. W celu realizacji powierzonych zadań ABI ma prawo:
   a) Kontrolować Komórki w Urzędzie Miejskim w Opocznie w zakresie właściwego zabezpieczenia systemów informatycznych, pomieszczeń, stanowisk pracy gdzie są przetwarzane dane osobowe.
   b) Wydawać polecenia Naczelnikom Wydziałów i Kierownikom komórek organizacyjnych w zakresie przestrzegania bezpieczeństwa danych osobowych.
   c) Informować Burmistrza Opoczna (ADO) o przypadkach naruszenia bezpieczeństwa danych osobowych.
   d) Żądania od wszystkich pracowników wyjaśnień w sytuacji naruszenia bezpieczeństwa danych osobowych

VII. Zasady udostępniania danych osobowych

§ 13

1. Urząd udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Zbiory danych udostępnia się na pisemny umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
3. Wniosek powinien zawierać informację umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
4. Wniosek jest rozpatrywany przez osobę upoważnioną przez ADO która jednocześnie prowadzi ich ewidencję.
5. Decyzję w sprawie udostępnienia danych osobowych podejmuje osoba upoważniona przez ADO.
6. Urząd może odmówić udostępnienia danych osobowych, jeżeli spowodowało by to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób

§ 14

1. Administrator Danych może powierzyć przetwarzanie danych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.
2. Podmiot o którym mowa w ust.1 jest zobowiązany do zastosowania środków organizacyjnych i technicznych zabezpieczających zbiór danych przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych i niniejszej dokumentacji.
3. W przypadkach opisanych w ust.1 i 2 , odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na AD co nie wyłącza odpowiedzialności podmiotu z którym zawarto umowę, z tytułu przetwarzania danych niezgodnie z umową.
4. Do kontroli zgodności przetwarzanych danych przez upoważniony przez AD podmiot, stosuje się odpowiednio przepisy art. 14-19 Ustawy o ochronie danych osobowych.

VIII. Obszar przetwarzania danych osobowych

§ 15

1. Obszarem przetwarzania danych osobowych w Urzędzie Miejskim w Opocznie są wszystkie pomieszczenia biurowe z wyłączeniem ciągów komunikacyjnych (korytarzy, klatek schodowych) oraz pomieszczeń sanitarnych i gospodarczych mieszczących się w budynkach przy ul. Staromiejskiej 6 w skład których wchodzą:
    a) Budynek A (parter i pietro)
    b) Budynek B (parter i pietro)
    c) Budynek C (parter i pietro)
    d) Budynek D (parter i pietro)
    e) Budynek E (parter i pietro)
    f) Budynek Główny (parter , pietro , piwnice)

g) Oficyna (Pomieszczenia Straży Miejskiej

2. Dane przetwarzane są również poza siedzibą główną Urzędu Miejskiego ,w Wydziale Promocji i Kultury zlokalizowanym w Miejskim Domu Kultury w Opocznie przy ul. Biernackiego 4. Pomieszczenia te mieszczą się na piętrze budynku i obejmują 2 pokoje.

§ 16

Komputery przenośne (Notebook) używane przez pracowników mogą być używane poza obszarem przetwarzania danych, jednakże osoby te muszą dołożyć wszelkich starań aby informacje zawarte na dyskach nie przedostały się do osób nieuprawnionych.

IX. Zabezpieczenie obszaru przetwarzania danych

§ 17

W ramach zabezpieczenia danych osobowych ochronie podlegają:

a) sprzęt komputerowy – serwery, komputery osobiste, notebooki, drukarki i inne urządzenia zewnętrzne,
b) oprogramowanie – kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne, licencjonowane nośniki danych,
c) dane zapisane na dyskach twardych, płytach CD i DVD, przenośnych pamięciach masowych(pendrive) oraz dane podlegające przetwarzaniu w systemie,
d) hasła użytkowników,
e) pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa,
f) użytkownicy i administratorzy, którzy obsługują system,
g) dokumentacja – zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje, itp.,
h) wydruki, związana z przetwarzaniem danych, dokumentacja papierowa, w których zawarte w nich dane są wprowadzane do systemu informatycznego lub też funkcjonują autonomicznie od niego.

§ 18

1. Zabezpieczenia fizyczne stosowane do zabezpieczenia danych osobowych w Urzędzie Miejskim w Opocznie to:

a) Całodobowy dozór pracownika obsługi nad budynkami Urzędu Miejskiego w Opocznie zlokalizowanymi przy ul. Staromiejskiej 6.
b) Budynek C w którym znajduje się Ewidencja Ludności wraz z Systemem Obsługi Dowodów Osobistych jest dodatkowo zabezpieczony systemem alarmowym. Hasła do systemu alarmowego przekazane są odpowiednim pracownikom którzy załączają i wyłączają system alarmowy.
c) Wszystkie pomieszczenia biurowe zamykane są na klucz. W każdym budynku zamontowane są metalowe drzwi z dwoma zamkami.
d) W budynkach A,B,C,D,E na parterze zamontowane są kraty w oknach.

e) Dokumenty dotyczące danych osobowych przechowywane są w szafach pancernych, szafach drewnianych, metalowych i biurkach z zamkami na klucz.

2. Zabezpieczenia fizyczne stosowane do zabezpieczenia danych osobowych w Wydziale Promocji i Kultury Urzędu Miejskiego w Opocznie , mieszczącym się w Miejskim Domu Kultury w Opocznie przy ul. Biernackiego 4:

   a) Pomieszczenia wydziału znajdują się na piętrze budynku w pokojach nr 23 i 24.
   b) Pietro budynku zabezpieczone jest dodatkowo kratami zamykanymi na klucz.
   c) Pomieszczenia te są zabezpieczone odpowiednimi drzwiami z podwójnym zamkiem.
   d) Poza godzinami pracy wydziału pomieszczenia te są zamykane a klucze przechowywane są w pomieszczeniu gospodarczym MDK.
   e) Klucze do pomieszczeń wydziału odbierają i zdają pracownicy wydziału.

3. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej to:

   a) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach
   b) przetwarzanie danych osobowych następuje przez wyznaczone i upoważnione do tego celu osoby

4. Zabezpieczenie organizacyjne to:

   a) osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Bezpieczeństwa Informacji (ABI),
   b) Administrator Bezpieczeństwa Informacji , Administrator Systemu Informatycznego oraz osoby upoważnione przez ABI na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,
   c) nie rzadziej, niż raz na tydzień są prowadzone przez ABI kontrole stanu bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony informacji i w przypadkach wykrycia rażących zaniedbań ABI sporządza ich opis w formie protokołu i raportu i niezwłocznie przedkłada je Burmistrzowi.

§ 19

1. Wszystkie pomieszczenia, które należą do obszaru przetwarzania danych, wyposażone są w odpowiednie zamki umożliwiające zamknięcie pomieszczeń celem niedostatnia się do nich osób nieupoważnionych.
2. W czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym.
3. Pracownicy opuszczając pomieszczenie w czasie godzin pracy są zobowiązani do zamykania ich na klucz i niedopuszczalne jest pozostawianie klucza w zamku drzwi.

3. Po skończonej pracy pracownicy zamykają drzwi na klucz i klucze przekazywane są osobie sprzątającej dany budynek.
4. Osoba sprzątająca budynek jest zobowiązana po zakończeniu pracy do zamknięcia wszystkich pomieszczeń biurowych i przekazania kluczy dla osoby dozorującej budynek. Przekazanie kluczy należy odnotować w rejestrze odbioru/zdawania kluczy.
5. Osoba dozorująca budynek jest zobowiązana do sprawdzenia wszystkich pomieszczeń pod kątem zamkniętych okien i drzwi.
6. Klucze przechowywane są w odpowiedniej gablocie zlokalizowanej w pomieszczeniu gospodarczym osób dozorujących.
7. Wydawanie Kluczy do pomieszczeń biurowych pracownikom następuje w godzinach od 6.45 do 7.30 we wszystkie dni robocze Urzędu.
8. Klucze wydaje osoba dozorująca przy podpisywaniu listy obecności.
9. Klucze mogą być wydawane tylko osobom pracującym w danych pomieszczeniach.
10. Osoba odbierająca klucze potwierdza odbiór w rejestrze odbioru/zdawania kluczy.
11. W dniach wolnych od pracy klucze mogą zostać wydane tylko w przypadku gdy pracownik został wpisany w odpowiedni rejestr znajdujący się w sekretariacie Urzędu.
12. Pracownik może zostać wpisany w rejestr zezwalający pracę po godzinach za zgodą i wiedzą Sekretarza Urzędu.

§ 20

1. Serwerownia jest miejscem, w którym przetwarzane są i przechowywane dane informatyczne całego Urzędu.
2. Pomieszczenie serwerowi jest klimatyzowane, celem utrzymania odpowiedniej temperatury dla zachowania prawidłowej pracy znajdujących się w niej urządzeń. Klimatyzacja w serwerowi działa w trybie automatycznym i włączana jest w razie potrzeby samoczynnie.
3. W oknie serwerowi zamontowane są żaluzje antywłamaniowe, które są zamykane po zakończeniu dnia pracy.
4. Pomieszczenie serwerowi jest zabezpieczone drzwiami antywłamaniowymi klasy C przeznaczonymi do zabezpieczenia pomieszczeń specjalnych.
5. Dostęp do serwerowi mają tylko Informatycy.
6. Po godzinach pracy urzędu serwerownia jest zamknięta bez możliwości dostępu osób nieupoważnionych.
7. Sprzątanie serwerowi następuje tylko i włącznie w obecności jednego z Informatyków w czasie godzin pracy.
8. Wszystkie osoby wchodzące do wejścia do serwerowi muszą posiadać zgodę ABI lub ASI i być wpisane do rejestru prowadzonego przez ASI.

§ 21

1. Wykaz pracowników Urzędzie Miejskim w Opocznie uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora Bezpieczeństwa Informacji.
2. Przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie wydawane przez Administratora Danych Osobowych,

3. W trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
4. Przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
5. W trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie, przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
6. Po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych,

§ 22

1. W systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim.
2. Najważniejszymi zastosowanymi środkami zabezpieczenia danych w systemach informatycznych w Urzędzie Miejskim w Opocznie są :
   a) hasła dostępu do komputera
   b) hasła dostępu do systemu,
   c) hasła dostępu do sieci komputerowej
   d) hasła dostępu do aplikacji,
   e) wygaszacze ekranu uaktywniane hasłem.

3. Dokumentem, który normuje procedury zarządzania systemem informatycznym służącym do przetwarzania danych osobowych jest Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Opocznie . Określa ona m.in.:

   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
   2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
   4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
   5) sposób, miejsce i okres przechowywania:
      a) elektronicznych nośników informacji zawierających dane osobowe,
      b) kopii zapasowych,
      c) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
   d) sposób realizacji wymogów odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,

e) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych
w Urzędzie Miejskim w Opocznie

Niniejszą instrukcję opracowano na podstawie §3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
Dotyczy wszystkich komputerów i systemów informatycznych przetwarzających dane osobowe w obszarze działania Urzędu Miejskiego w Opocznie.

1 Pojęcia

1.1 Ustawa — rozumie się przez to ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z poźn. zm.).

1.2 Administrator Danych Osobowych (ADO) – rozumie się przez to organ, instytucję, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ust. 1 i 2, decydujące o celach i środkach przetwarzania danych osobowych. W Urzędzie Miejskim w Opocznie administratorem danych osobowych w rozumieniu przepisów ustawy jest Burmistrz Opoczna.

1.3 Administrator Bezpieczeństwa Informacji (ABI) – osoba powołana Zarządzeniem nr 4/2001 Burmistrza Miasta Opoczna z dnia 19 listopada 2001, która odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym Urzędu, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

1.4 Administrator Systemu Informatycznego (ASI) - osoba upoważniona przez Administratora Bezpieczeństwa Informacji – administrator konkretnego systemu informatycznego przetwarzającego dane osobowe.

1.5 Dane osobowe - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

1.6 Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

1.7 Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.

1.8 System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

1.9 Identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

1.10 Hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

1.11 Uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

1.12 Integralność danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

1.13 Poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

1.14 Konto poczty służbowej – elektroniczne konto pocztowe utworzone na wirtualnym serwerze Urzędu Miejskiego charakteryzujące się nazwą@um.opoczno.pl.

1.15 „niezaufany” nadawca poczty elektronicznej - rozumie się przez to nieznanego nam nadawcę, nie dającego się zidentyfikować na podstawie adresu poczty, adresu nie będącego adresem poczty służbowej, nadawcę wiadomości nie zawierającej żadnej treści lub zawierającego treści reklamowe w różnej postaci.

2 Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

2.1 Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez ABI.

2.2 Ewidencje upoważnień do przetwarzania danych osobowych, o których mowa w punkcie 2.1, prowadzi ABI.

2.3 Rejestracji użytkownika systemu informatycznego dokonuje się na podstawie upoważnienia, o którym mowa w punkcie 2.1.

2.4 Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła.

2.5 Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Bezpieczeństwa Informacji ustala niepowtarzalny identyfikator i hasło początkowe.

2.6 Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.

2.7 Administrator Bezpieczeństwa Informacji wyznacza dla systemu informatycznego, Administratora Systemu Informatycznego oraz osobę zastępującą w przypadku jego nieobecności. Administratorowi Systemu Informatycznego przydziela się w systemie identyfikator użytkownika uprzywilejowanego.

2.8 Naczelnik Wydziału lub Kierownik komórki organizacyjnej Urzędu, w ramach której działa podległy mu użytkownik informuje Administratora Bezpieczeństwa Informacji o fakcie utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest Administrator Systemu Informatycznego.

2.9 Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona przekazując użytkownikowi identyfikator i hasło przeprowadza szkolenie z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.

2.10 Ewidencje użytkowników każdego systemu informatycznego przetwarzającego dane osobowe prowadzi Administrator Bezpieczeństwa Informacji. Za aktualizację ewidencji użytkowników odpowiedzialny jest Administrator Systemu Informatycznego.

3 Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

3.1 Dane osobowe przetwarzane są w Urzędzie Miejskim w Opocznie z użyciem dedykowanych serwerów, komputerów stacjonarnych i przenośnych.

3.2 Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane co 90 dni.

3.3 Hasło oprócz znaków małych i dużych liter winno zawierać ciąg znaków alfanumerycznych i specjalnych.

3.4 Administrator Bezpieczeństwa Informacji nadaje hasło początkowe i wymusza w systemie zmianę haseł użytkowników.

3.5 Na wydzielonych stanowiskach komputerowych (nie pracujących w ramach sieciowego systemu informatycznego),oraz w systemach, w których automatyczne wymuszenie zmiany hasła nie następuje, hasło powinno być zmieniane nie rzadziej niż raz na 90 dni. Za jego zmianę odpowiedzialny jest użytkownik.

3.6 Stanowiska komputerowe na których skonfigurowanie identyfikatora i hasła zapewniającego ochronę jest nieskuteczne, zabezpiecza się dodatkowym hasłem (hasło wygaszacza ekranu, hasło BIOSu)

3.7 Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej.

3.8 Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.

3.9 Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej.

3.10 Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności.

3.11 Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.

3.12 Hasła Administratorów Systemu Informatycznego są zdeponowane w Sejfie w Wydziale Organizacyjnym Urzędu Miejskiego w Opocznie.

3.13 Użytkownik otrzymuje hasło początkowe przy przystąpieniu do pracy w systemie i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy na tylko sobie znany ciąg znaków. Administrator Bezpieczeństwa Informacji lub wyznaczona przez niego osoba – Administrator Systemu Informatycznego zobowiązana jest dopilnować lub wymusić w systemie zmianę haseł początkowych.

3.14 W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

3.15 W przypadku przetwarzania danych na komputerach przenośnych, dyski twarde oraz inne wykorzystywane nośniki informacji mają być zabezpieczone w sposób uniemożliwiający dostęp do tych danych osobom postronnym (np. nieuprawniony dostęp, kradzież komputera, szpiegostwo przemysłowe), poprzez wykorzystanie metod i środków kryptograficznych (szyfrowane partycje dysków twardych, szyfrowanie plików, ochrona fizyczna nośników).

4 Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

4.1 Dane osobowe, których administratorem jest Burmistrz Opoczna, mogą być przetwarzane z użyciem systemu informatycznego tylko na potrzeby realizowania zadań ustawowych i organizacyjnych.

4.2 Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).

4.3 Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji lub w przypadku braku takiej w dokumentacji wg wskazówek i szkolenia przeprowadzonego przez ASI.

4.4 Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji, w przypadku braku takiej w dokumentacji wg wskazówek i szkolenia przeprowadzonego przez ASI.

4.5 Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.

4.6 System po upływie 10 minut braku aktywności ze strony użytkownika automatycznie blokuje dostęp do konsoli. Ponowne jego odblokowanie możliwe jest po podaniu hasła. W przypadku braku możliwości realizacji ww. funkcjonalności monitory ekranowe stanowisk, na których przetwarzane są dane osobowe po 10 minutach nieaktywności użytkownika, powinny przejść automatycznie w stan nieaktywny, a powrót do stanu aktywności musi wymagać podania hasła.

4.7 Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, o których mowa w punkcie 2.1, a na których przetwarzane są dane osobowe należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.

4.8 Użytkownik ma obowiązek wylogowania się z lub zablokowania systemu w przypadku dłuższej, zaplanowanej nieobecności na stanowisku pracy lub w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika.

4.9 Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie (niszczarka dokumentów).

4.10 Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.

4.11 Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.

4.12 Użytkownik niezwłocznie powiadamia Administratora Systemu Informatycznego w przypadku braku możliwości zalogowania się na swoje konto oraz Administratora Bezpieczeństwa Informacji w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

5 Procedura monitorowania i audytu sieci komputerowej

5.1 W sieci komputerowej Urzędu Miejskiego w Opocznie zainstalowane jest oprogramowanie do monitoringu sieci.

5.2 Oprogramowanie to ma za zadanie prowadzenie:

5.2.1 Audytu legalności - oprogramowania, kontrola zainstalowanego oprogramowania na danym stanowisku roboczym,

5.2.2 Inwentaryzacji sprzętu komputerowego, sprawdzania wszystkich parametrów zestawu komputerowego użytkownika,

5.2.3 Kontrola czasu pracy na stanowisku komputerowym, wydruku i statystyk obrazujących efektywny czas pracy użytkownika na poszczególnych aplikacjach i procesach. Czas liczony jest na podstawie efektywnego wykorzystania komputera a nie procesu zrzuconego na pasek zadań,

5.2.4 Kontrola aktywności pracy użytkowników, wydruki i statystyki obrazujące efektywny czas pracy użytkownika na poszczególnych aplikacjach i procesach. Czas liczony jest na podstawie efektywnego wykorzystania komputera a nie procesu zrzuconego na pasek zadań,

5.2.5 Zarządzanie siecią komputerową poprzez przejęcie kontroli stanowiska komputerowego i dokonanie na nim operacji niezbędnych do prawidłowej pracy.

5.3 Oprogramowanie to jest zainstalowane na wszystkich komputerach w Urzędzie

5.4 Po zalogowaniu się użytkownik otrzymuje komunikat potwierdzający, że dany komputer jest monitorowany

5.5 Wszystkie statystyki i informacje o czasie pracy, aktywności, odwiedzanych stronach w każdym momencie są do wglądu i do wydruku.

6 Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania

6.1 Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:

6.1.1 urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,

6.1.2 sporządzania kopii zapasowych zbiorów danych (kopie pełne).

6.2 Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego lub osoba wyznaczona przez Administratora Bezpieczeństwa Informacji.

6.3 Pełne kopie zapasowe zbiorów danych są tworzone codziennie

6.4 W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.

6.5 Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Systemu Informatycznego.

6.6 Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

7 Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

7.1 Okresowe kopie zapasowe wykonywane są na dyskietkach, płytach CD, DVD, taśmach lub innych elektronicznych nośnikach informacji. Kopie powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikację, uszkodzenie lub zniszczenie.

7.2 Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Administrator Bezpieczeństwa Informacji oraz Administrator danego Systemu Informatycznego, którego kopie zawierają konkretne nośniki.

7.3 Kopie miesięczne przechowuje się przez okres 3 miesięcy. W przypadku danych finansowo - księgowych okres przechowywania danych wynosi 5 lat. Wykonywane co pół roku pełne kopie systemu kadrowo-płacowego przechowuje się przez 5 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.

7.4 Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.

7.5 W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.

7.6 W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.

7.7 W przypadku braku możliwości zrealizowania procedury zniszczenia nośników informacji, należy fakt ten zgłosić Administratorowi Bezpieczeństwa Informacji lub Administratorowi Systemu Informatycznego. Po przekazaniu nośników zostaną one zniszczone w ramach środków technicznych Komórki Informatycznej, bądź poddane procedurze utylizacji nośników informacji realizowanej przez firmę zewnętrzną.

8 Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

8.1 W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych oraz oprogramowania złośliwego typu malware, spyware, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.

8.2 Wirusy komputerowe oraz wyżej wymienione oprogramowanie mogą pojawić się w systemach Urzędu poprzez: Internet, nośniki informacji takie jak: dyskietki, płyty CD, DVD, dyski przenośne, pamięci typu flash itp.

8.3 Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych i szkodliwemu oprogramowaniu realizowane jest następująco:

8.3.1 Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego i anty malware i spyware.

8.3.2 Informatycy zobowiązani są do dopilnowania, aby zainstalowany program antywirusowy był tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych oraz oprogramowania złośliwego.

8.3.3 Elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, pamięci typu flash itp. należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Systemu Informatycznego, bądź powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

8.3.4 Komputery i systemy pracujące w Urzędzie muszą mieć zainstalowany program antywirusowy a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).

8.3.5 W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Systemu Informatycznego, Administratorem Bezpieczeństwa Informacji lub Informatykiem.

8.4 Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych” nadawców.

8.5 Zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

9 Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

9.1 Udostępnienie danych osobowych instytucjom, osobom może odbywać się wyłącznie na pisemny uzasadniony wniosek, za pośrednictwem Administratora Danych Osobowych lub osoby przez niego upoważnionej.

9.2 Ewidencję udostępniania danych osobowych prowadzi osoba upoważniona przez ADO.

10 Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

10.1 Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator Systemu Informatycznego lub osoba wyznaczona przez Administratora Bezpieczeństwa Informacji na bieżąco, lecz nie rzadziej niż raz w miesiącu. Sprawdzana jest spójność danych, indeksów oraz stan nośników informacji, np. dysków twardych oraz urządzeń peryferyjnych.

10.2 Administrator Systemu Informatycznego okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest ustalana przez Administratora Bezpieczeństwa Informacji.

10.3 Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku.

10.4 Naprawy serwisowe sprzętu objętego umowami serwisowymi odbywać się będą zgodnie z umową. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz wyznaczonego przez Administratora Bezpieczeństwa Informacji pracownika , w miejscu jego użytkowania.

10.5 W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.

10.6 Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.

11 Ustalenia końcowe

11.1 Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w Urzędzie zabrania się:

a. ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,

b. pozostawiania haseł w miejscach widocznych dla innych osób,

c. udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,

d. udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,

e. używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,

f. przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,

g. kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza Urząd,

h. samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez Administratora Systemu Informatycznego lub za jego zgodą, na polecenie Administratora Bezpieczeństwa Informacji, przez inną upoważnioną osobę, po uprzednim ich przetestowaniu i sprawdzeniu,

i. używania nośników danych udostępnionych przez osoby postronne,

j. przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (nie służbowego),

k. otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych” nadawców,

l. używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia - przeskanowania programem antywirusowym, Informatykom Administratorowi Bezpieczeństwa Informacji lub osobie przez niego upoważnionej,

m. wykorzystywania sieci komputerowej w celach innych, niż określone w Regulaminie sieci komputerowej Urzędu Miejskiego w Opocznie,

n. tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania,

o. narażania sprzętu i nośników danych na kradzież (w tym: pozostawienie komputera przenośnego w miejscu publicznym, w samochodzie itp. bez zabezpieczenia).

11.2 Ponadto zabrania się:

a. wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,

b. pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach lub centrach wydruku,

c. pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,

d. pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach Urzędu, w których przetwarzane są dane osobowe,

e. pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,

f. ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,

g. przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,

h. ignorowania zapisów Polityki Bezpieczeństwa Informacji Urzędu Miejskiego w Opocznie.

11.3 Konieczne jest:

a. posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,

b. tworzenia haseł trudnych do odgadnięcia dla innych,

c. traktowanie konta pocztowego Urzędu jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,

d. nie przerywanie procesu skanowania przez program antywirusowy na komputerze,

e. wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,

f. zaprowadzenie porządku w zakresie organizacji plików w systemie ułatwiającego przeprowadzenie procesu archiwizacji danych ,

g. zabezpieczenie sprzętu komputerowego w tym komputerów przenośnych przed kradzieżą lub nieuprawnionym dostępem do danych.

11.4 Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa Informacji lub bezpośredniemu przełożonemu.

11.5 Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązały się do przestrzegania zasad w nim zawartych.

11.6 Dane kontaktowe

a. Administrator Bezpieczeństwa Informacji – Urząd Miejski w Opocznie ul. Staromiejska, tel. (044)7363103, abi@um.opoczno.pl

Załącznik. Nr 3
Do Dokumentacji Systemu
Zarządzania Bezpieczeństwem Informacji
w Urzędzie Miejskim w Opocznie

Instrukcja
postępowania w sytuacji naruszenia ochrony danych osobowych w systemach informatycznych Urzędu Miejskiego w Opocznie

Opracował: Administrator Bezpieczeństwa Informacji inż. Dariusz Badura
UM Opoczno Grudzień 2008

I. Opis zdarzeń naruszających ochronę danych osobowych

1. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   b) niewłaściwe parametry środowiska, np. niewłaściwa wilgotność, temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje,
   c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub sabotaż,
   d) niewłaściwe działanie serwisu, w tym także pozostawienie serwisantów bez nadzoru,
   e) pojawienie się komunikatu alarmowego pochodzącego od części systemu zapewniającej ochronę zasobów lub innego komunikatu o podobnym znaczeniu,
   f) zła jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego, wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   g) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   h) stwierdzenie modyfikacji danych, próby ich modyfikacji lub zmiany w strukturze danych bez upoważnienia,
   i) stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie informatycznym,
   j) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania lub innych chronionych elementów systemu zabezpieczeń,
   k) funkcjonowanie systemu lub jego sieci komputerowej wykazujące odstępstwa od założonego rytmu pracy, uprawdopodobniające przełamanie lub zaniechanie ochrony danych osobowych, np. praca przy komputerze lub w sieci osoby, która nie jest dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
   l) obecność w obszarze przetwarzania danych osobowych osób postronnych bez dozoru pracowników zatrudnionych przy przetwarzaniu danych osobowych,
   m) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
   n) podmiana lub zniszczenie nośników z danymi osobowymi bez zachowania procedury; skasowanie lub skopiowanie danych osobowych w sposób niedozwolony,
   o) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie wydrukowanych danych osobowych w drukarce czy w kserografie, niewykonanie w określonym terminie kopii bezpieczeństwa, itp.).

2. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przetwarzania danych osobowych, itp. pozostawienie otwartego pomieszczenia w obszarze bezpieczeństwa; umożliwienie nieautoryzowanego dostępu do urządzeń archiwizujących itp.

II. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:
   a) zabezpieczenia systemu informatycznego,
   b) stanu urządzeń,
   c) zawartości zbioru danych osobowych,
   d) wynikającego z ujawnienia metody pracy lub sposobu działania programu,
   e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. pożar itp.)

   każdy pracownik/użytkownik systemu zatrudniony przy przetwarzaniu danych osobowych jest obowiązany niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji lub Administratora Systemów Informatycznych.

2. Pracownicy/Użytkownicy systemu, którzy stwierdzili naruszenie ochrony danych osobowych, o których mowa w pkt. 4 i 5 w oczekiwaniu na przebycie ABI muszą:
   a) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   b) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   c) wstrzymać bieżącą pracę w celu zabezpieczenia miejsca zdarzenia,
   d) zaniechać, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   e) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   f) udokumentować wstępnie zaistniałe naruszenie,
   g) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

3. Po przybyciu na miejsce naruszenia ochrony danych osobowych ABI:
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze wnioski z przeprowadzonych wcześniej symulacji zagrożeń oraz politykę bezpieczeństwa w tym zakresie,
   b) żąda dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

4. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien w szczególności zawierać:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia i powiadomienia,

c) określenie rodzaju naruszenia i okoliczności towarzyszących,
d) opis podjętego działania i metody postępowania,
e) wstępną ocenę przyczyn wystąpienia naruszenia,
f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

5. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. Zaistniałe naruszenie powinno stać się przedmiotem szczegółowej, zespołowej analizy z udziałem Naczelnika wydziału, ABI i administratora systemu.

7. Analiza, o której mowa w pkt. 7, powinna zawierać wszechstronna ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości. ABI przedstawia analizę Burmistrzowi Opoczna.

III. Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszej Instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej procedury mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez pracownika, który wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomił o tym ABI.

REGULAMIN sieci komputerowej Urzędu Miejskiego w Opocznie

§ 1

Regulamin sieci komputerowej Urzędu Miejskiego w Opocznie, zwany dalej „Regulaminem" ma zastosowanie do sieci komputerowej zlokalizowanej na terenie Urzędu Miejskiego przy ulicy Staromiejskiej 6 obejmującej swoim zasięgiem wszystkie budynki Urzędu . Oznaczenie sieci w skrócie to „SUMO"

§ 2

Użyte w Regulaminie określenia oznaczają:

1. sieć — lokalna sieci komputerowe obejmujące środki sprzętowe i programowe umożliwiające realizację połączeń między stacjami roboczymi i serwerami sieci w SUMO,
2. stacja robocza — komputer podłączony do sieci jako jej urządzenie końcowe, służący do bezpośredniego wspomagania pracy użytkownika sieci;
3. użytkownik sieci — upoważniona osoba korzystającą ze stacji roboczej lub przesyłającą informacje poprzez sieci niezależnie od lokalizacji stacji roboczej, z której korzysta,
4. administrator sieci — upoważnionego przez Burmistrza Opoczna osoba, realizującego zadania w zakresie eksploatacji sieci, serwerów i stacji roboczych;
5. Regulamin organizacyjny SUMO — załącznik do Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie wprowadzony zarządzeniem Burmistrza Nr ……..
6. Wydział — komórki organizacyjne Urzędu Miejskiego
7. urządzenia peryferyjne — urządzenia zewnętrzne komputera takie, jak drukarki, monitory, skanery i inne.

§ 3

Sieć umożliwia:

1. przesyłanie i udostępnianie zbiorów danych (plików i baz danych);
2. przesyłanie i odbiór poczty elektronicznej;
3. wykonywanie innych czynności wynikających z aktualnych charakterystyk techniczno-eksploatacyjnych sieci.

§ 4

1. Administrator sieci:

- jest zobowiązany zapewnić sprawne , efektywne i bezpieczne funkcjonowanie sieci,
- przydziela i rejestruje adresy sieciowe oraz nazwy wszystkich serwerów i stacji roboczych;
- nadzór nad serwerami usług internetowych, takich jak: serwery pocztowe, serwery ftp, WWW;
- sprawuje nadzór techniczny nad sprzętem sieciowym;
- zarządza kontami użytkowników sieci
- zarządzanie kontami poczty elektronicznej
- prowadzi nadzór nad sprzętem i oprogramowaniem zainstalowanym na stacjach roboczych użytkowników;
- konserwuje i naprawia sprzęt komputerowy;
- pomaga użytkownikom w naprawach i rozwiązywaniu problemów;
- prowadzi nadzór techniczny nad sprzętem komputerowym.
- jest zobowiązany zapewnić sprawne, efektywne i bezpieczne funkcjonowanie właściwej sobie bazy danych.

2. Zmian konfiguracji urządzeń wchodzących w skład sieci albo zmian konfiguracji oprogramowania sieciowego może dokonywać administrator sieci.

§ 5

1. Prawo do korzystania z sieci oraz ze stacji roboczych przysługuje:
   - pracownikom Urzędu,
   - osobom upoważnionym przez Burmistrza lub Administratora Bezpieczeństwa Informacji,

2. Konto lub konta użytkownika sieci na serwerach włączonych do sieci są zakładane na wniosek właściwego Naczelnika Wydziału, sporządzony na formularzu określonym przez administratora sieci.

3. Konto lub konta użytkownika sieci na serwerach włączonych do sieci są usuwane:
   - na uzasadniony pisemny wniosek właściwego naczelnika wydziału
   - po otrzymaniu informacji o rozwiązaniu z pracownikiem umowy o pracę lub wygaśnięciu upoważnienia, o którym mowa w pkt. 1— pod warunkiem zarchiwizowania znajdujących się na koncie plików.

§ 6

Uprawnienia i obowiązki użytkownika

1. Użytkownik sieci ma prawo do korzystania z sieci, w zakresie określonym w § 3, w tym do korzystania z zasobów serwerów, na których ma założone konto, zgodnie z uprawnieniami określonymi przez administratora sieci.

2. Użytkownik sieci jest obowiązany należycie dbać o sprzęt.

3. Użytkownik sieci jest obowiązany kontrolować dostęp do stacji roboczej, którą użytkuje i nie pozostawiać bez nadzoru stacji roboczych zalogowanych do sieci (z otwartą sesją).

4. Użytkownik sieci jest obowiązany należycie zabezpieczyć poufność danych umożliwiających dostęp do własnego konta, w szczególności hasła.

5. Komputer należy zabezpieczyć wygaszaczem ekranu zabezpieczonym hasłem (max. 10 min).

6. Użytkownik sieci ma obowiązek stosowania się do zaleceń administratora sieci, w sprawach dotyczących bezpieczeństwa i efektywności eksploatacji stacji roboczych, które użytkuje, a zwłaszcza do:
    - *zakazu* instalacji jakiegokolwiek oprogramowania bez wiedzy i pisemnej zgody administratora sieci (zgoda na instalację oprogramowania może być przekazana drogą elektroniczną);
    - zakazu przenoszenia i samodzielnej instalacji sprzętu komputerowego.

7. W przypadku korzystania ze wspólnych urządzeń peryferyjnych użytkownik ma prawo włączyć, a następnie wyłączyć stację roboczą udostępniającą to urządzenie.

8. Po skończonej pracy należy wyłączyć komputer i urządzenia peryferyjne.

§ 7

Zabronione w sieci komputerowej jest:

1. Zabrania się dokonywania działań mających na celu uzyskanie nieupoważnionego dostępu do konta innego użytkownika sieci lub do innych zasobów zgromadzonych na serwerach w sieciach, w szczególności podszywania się pod innych użytkowników sieci lub monitorowania łącz.

2. W razie wykrycia działań, o których mowa w punkcie l, administrator sieci może zablokować konto lub konta użytkownika sieci, powiadamiając o tym swojego przełożonego.

3. Zabrania się wykonywania, bez uzgodnienia z administratorem sieci, czynności mogących w istotny sposób zakłócić funkcjonowanie sieci, a w szczególności rozłączania okablowania, wymiany sprzętu lub instalowania telefonicznych połączeń modemowych

4. Zabrania się wykorzystywania sieci do celów zarobkowych, w tym do rozsyłania nie zamówionych informacji handlowych, w rozumieniu przepisów o świadczeniu usług drogą elektroniczną.

5. Używanie stacji roboczych w celach prywatnych, niezwiązanych z wykonywaniem obowiązków

służbowych możliwe jest tylko w uzasadnionych przypadkach, zgodnie z obowiązującymi w tym zakresie przepisami i za zgodą bezpośredniego przełożonego.

§ 8

1. Za świadome dopuszczenie do korzystania z sieci osób prowadzących działalność zarobkową odpowiada dyscyplinarnie administrator sieci i użytkownik stacji roboczej, z której ta działalność była prowadzona.
2. W przypadku nieupoważnionego korzystania z konta użytkownika sieci do celów zarobkowych, administrator może zablokować konto lub konta użytkownika sieci, powiadamiając o tym swojego przełożonego.

§ 9

Administrator sieci nie ponosi odpowiedzialności za naruszenia prywatności lub bezpieczeństwa zbiorów danych powstałe z winy użytkownika sieci, w szczególności wskutek udostępnienia hasła osobom nieuprawnionym.

§ 10

Prawa administratorów.

1. Administrator sieci (oprogramowanie, bazy danych) w odniesieniu do tych zasobów, mogą ograniczyć możliwości wykonywania przez wszystkich lub niektórych użytkowników sieci pewnych operacji (uruchamianie programów, odczyt albo zapis zbiorów danych, nawiązywanie połączeń z innymi systemami itp.), o ile jest to uzasadnione względami technicznymi albo wynika z odrębnych przepisów lub postanowień niniejszego Regulaminu.

2. Administratorzy bazy danych mogą ograniczyć możliwości wykonywania przez wszystkich lub niektórych użytkowników sieci pewnych operacji na bazie danych , o ile jest to uzasadnione względami bezpieczeństwa bazy danych albo wynika z odrębnych przepisów lub postanowień niniejszego Regulaminu.

3. Bezpośredni dostęp do każdego zbioru danych utworzonego przez użytkownika sieci posiada administrator sieci, który może dokonywać kontroli w zakresie realizacji postanowień zawartych w ust. 5.

4. Administrator sieci może dokonywać na zbiorach danych utworzonych przez użytkowników sieci operacji wymaganych do zachowania sprawnego i bezpiecznego działania sieci lub serwerów, jednak nie może ingerować w treść tych zbiorów.

§ 11

Obowiązki administratorów

1. Administrator sieci informuje użytkownika sieci o przysługujących mu możliwościach korzystania z sieci i jej zasobów oraz o ewentualnych problemach związanych z jej eksploatacją, a zwłaszcza o obowiązku oraz sposobie i częstotliwości zmiany haseł.

2. Administrator sieci informuje użytkownika bazy o przysługujących mu możliwościach korzystania z podległej mu bazy danych oraz o ewentualnych problemach związanych z jej eksploatacją.

3. Administrator sieci udostępnia nr telefonu wew. 103, w celu zgłaszania przez użytkowników sieci problemów związanych z eksploatacją sieci, stacji roboczych i usługami sieciowymi.

4. Administrator sieci prowadzi szkolenia, w zakresie dostępnych aplikacji i baz danych.

5. Administrator sieci, na uzasadniony wniosek właściwego naczelnika wydziału, ma obowiązek udostępnić zbiory danych utworzonych w związku z wykonywaniem obowiązków pracowniczych użytkownika sieci, jeśli są one niezbędne do zachowania toku pracy tej komórki organizacyjnej i nie jest możliwy dostęp do tych zbiorów danych w inny sposób.

6. Administrator bazy danych, na uzasadniony wniosek właściwego naczelnika wydziału lub osoby upoważnionej przez ABI, ma obowiązek udostępnić zbiory danych , jeśli są one niezbędne do zachowania toku pracy tej komórki organizacyjnej.

7. Administrator sieci i inne osoby upoważnione mające dostęp do zbiorów danych utworzonych przez innych użytkowników sieci, obowiązane są przestrzegać tajemnicy korespondencji oraz zasad ochrony informacji niejawnych w odniesieniu do udostępnionych im zbiorów danych.

8. Administrator sieci prowadzi rejestr wszystkich użytkowników mających dostęp do zasobów sieciowych według załącznika nr 2 do niniejszego regulaminu.

§ 12

1. Naczelnik Wydziału zapoznaje z niniejszym Regulaminem każdego pracownika kierowanej przez siebie komórki organizacyjnej, będącego użytkownikiem sieci.

2. Po zapoznaniu z regulaminem użytkownik sieci podpisuje oświadczenie, stanowiące załącznik nr 1 do Regulaminu sieci komputerowej. Oryginał podpisanego oświadczenia, opatrzonego datą, należy przekazać do administratora sieci.

3. Naczelnik Wydziału informuje administratora sieci o zakresie uprawnień użytkownika do poszczególnych systemów i programów oraz ewentualnych zmianach tych uprawnień(w szczególności w przypadku ich odebrania). Zakres uprawnień zostaje wyszczególniony na formularzu administratora sieci i

po podpisaniu przez Naczelnika Wydziału przekazany administratorowi sieci.

§ 13

Wszystkie zmiany konfiguracyjne i konserwacyjne świadczone przez firmy zewnętrze a mające wpływ na działanie sieci lub oprogramowania w niej udostępnionego muszą być zgłaszane administratorowi sieci lub administratorowi lokalnych zasobów komputerowych i przez niego nadzorowane.

§ 14

Sieć komputerowa jest monitorowana pod kątem instalowanego oprogramowania, inwentaryzacji sprzętu komputerowego, efektywnego ruchu do Internetu jak również czasu pracy pracowników.

Załącznik nr 1
do Regulaminu Sieci komputerowej
Urzędu Miejskiego w Opocznie

Opoczno, dn. ……

Imię i nazwisko ……

Stanowisko służbowe ……

Komórka organizacyjna ……

Telefon ……

Oświadczenie

Oświadczam, że znane mi są zasady korzystania z sieci komputerowej określone w Regulaminie sieci komputerowej Urzędu Miejskiego w Opocznie.

Jestem świadomy, że nieprzestrzeganie postanowień niniejszego Regulaminu skutkuje pociągnięciem do odpowiedzialności dyscyplinarnej, zgodnie z obowiązującym Przepisami Prawa Pracy.

Podpis pracownika

Adnotacje przełożonych:

Załącznik nr.2
do Regulaminu Sieci komputerowej
Urzędu Miejskiego w Opocznie

Opoczno, dn. ……

Imię i nazwisko ……

Stanowisko służbowe ……

Komórka organizacyjna ……

Nr Pokoju ……

Zakres uprawnień użytkownika do programów i systemów

1.	**Nazwa Programu Systemu, Serwera**	**Data nadania uprawnie**ń	**Nazwa konta i zakres uprawnie**ń**(odczyt/zapis/pełne/inne)**	**Data odebrania uprawnie**ń
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

11.				
12.				
13.				
14.				
15.				
16.				
17.				

Podpis administratora sieci

Adnotacje administratora

Nazwa Komputera ……

MAC adres stacji roboczej ……

Adres IP komputera ……

WZÓR Załącznik. Nr 5
Do Dokumentacji Systemu
Zarządzania Bezpieczeństwem Informacji
w Urzędzie Miejskim w Opocznie

OŚWIADCZENIE

Ja niżej podpisana/ny …….. zobowiązuje się do zachowania w tajemnicy danych osobowych, do których mam dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Urzędzie Miejskim w Opocznie , zarówno w trakcie obecnego stosunku pracy jak również po ustaniu zatrudnienia.

Ponadto:

1. Oświadczam, że znana jest mi definicja danych osobowych w rozumieniu art. 6 Ustawy o ochronie danych osobowych z dnia 29.08.1997r. (Dz. U. 2002 r.101.926 z późn. zm.) w myśl, której za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, z Dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Opocznie w zakresie przetwarzania danych osobowych w Urzędzie Miejskim w Opocznie i zobowiązuje się do przestrzegania zapisów tego dokumentu.
3. Zobowiązuję się, w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub Sekretarza Miasta .
4. Zobowiązuję, się przy przetwarzaniu danych osobowych, do szczególnej dbałości o zachowanie poufności, integralności i dostępności danych związanych z dokumentami znajdującymi się w obrocie w Urzędzie, także dotyczących danych osobowych pracowników, dokumentacji systemu przetwarzania danych oraz infrastruktury sprzętowo - programowej systemów informatycznych.
5. Zobowiązuję się przy przetwarzaniu danych, poza systemem informatycznym, do szczególnej dbałości o zachowanie poufności treści dokumentów, które znajdują się w obrocie w Urzędzie oraz przestrzegania zasad dostępu do danych osobowych.
6. Oświadczam, że przyjmuje do wiadomości , iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

……
podpis pracownika

WZÓR

Załącznik Nr 6
Do Dokumentacji Systemu
Zarządzania Bezpieczeństwem Informacji
w Urzędzie Miejskim w Opocznie

Data nadania upoważnienia: .....

Upoważnienia do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926, z późn.zm.)

upoważniam Panią/Pana .....
(imię i nazwisko upoważnianego)
zatrudnioną/-ego na stanowisku .....
w .....
(wpisać nazwę administratora - pracodawcy)

do dostępu do danych osobowych wynikających z zakresu zadań wykonywanych na zajmowanym stanowisku, a w szczególności**:**

1) .....
2) .....
3) .....
4) ……..….

(należy sprecyzować zakres upoważnienia; można go określić poprzez wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba lub rodzaj czynności lub operacji, jakich może ona dokonywać na danych osobowych – o ile tylko administrator uzna to za stosowne)

Nadaję Identyfikator:
.....
(wypełnia się jedynie w przypadku, gdy dane przetwarzane są w systemie informatycznym)

Okres trwania upoważnienia:
.....
(należy sprecyzować okres obowiązywania upoważnienia, np. od dnia wystawienia do chwili ustania stosunku pracy)

Wystawił: .....
(podpis administratora
lub osoby reprezentującej administratora)

Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

WZÓR

Załącznik. Nr 7
Do Dokumentacji Systemu
Zarządzania Bezpieczeństwem Informacji
w Urzędzie Miejskim w Opocznie

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do ....
(dokładne oznaczenie administratora danych)

2. Wnioskodawca ....
(nazwa firmy i jej siedziba albo imię, nazwisko i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust. 1 ustawy o chronie danych osobowych:

.....

❒ ew. cd. w załączniku nr …...

4. Wskazanie przeznaczenia dla udostępnionych danych: .....

....

❒ ew. cd. w załączniku nr …...

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane: …….....

……..... .....

6. Zakres żądanych informacji ze zbioru: ....

……..... .....

❒ ew. cd. w załączniku nr ……..

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych: .....

....

❒ ew. cd. w załączniku nr ……..

* Jeżeli TAK, to zakreśl kwadrat literą "X".
(miejsce na znaczki opłaty skarbowej)

.....
(data, podpis i ew. pieczęć wnioskodawcy)