Zarządzenie Nr 78/2012
Burmistrza Sulejowa
z dnia 10 lipca 2012 roku

w sprawie wprowadzenia w Urzędzie Miejskim „Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych ”, „Polityki bezpieczeństwa”, „Instrukcji określającej prawa i obowiązki użytkowników sprzętu komputerowego”, „Instrukcji w sprawie zasad postępowania w sytuacji naruszenia ochrony danych osobowych”, „Instrukcji postępowania w sprawie zabezpieczenia zbiorów danych przed pożarem, zalaniem i innym niebezpieczeństwem grożącym zniszczeniem lub utratą zbiorów.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zmianami) §3, §4 i §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100 poz. 1024) oraz §24 Regulaminu organizacyjnego Urzędu Miejskiego, stanowiącego załącznik do Zarządzenia Nr 79/2005 z dnia 30 grudnia 2005 r.

zarządzam, co następuje:

§1. Wprowadza się do stosowania i przestrzegania w Urzędzie Miejskim w Sulejowie:

1) **Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**, stanowiącą Załącznik Nr 1 do niniejszego Zarządzenia.
2) **Politykę bezpieczeństwa**, stanowiącą Załącznik Nr 2 do niniejszego Zarządzenia.
3) **Instrukcję określającą prawa i obowiązki użytkowników sprzętu komputerowego,** stanowiącą Załącznik Nr 3 do niniejszego Zarządzenia.
4) **Instrukcję w sprawie zasad postępowania w sytuacji naruszenia ochrony danych osobowych,** stanowiącą Załącznik Nr 4 do niniejszego Zarządzenia.
5) **Instrukcję postępowania w sprawie zabezpieczenia zbiorów danych w** Urzędzie Miejskim w Sulejowie **przed pożarem, zalaniem i innym niebezpieczeństwem grożącym zniszczeniem lub utratą zbiorów**, stanowiącą Załącznik Nr 5 do niniejszego Zarządzenia.

§2. Zobowiązuję wszystkich pracowników Urzędu Miejskiego do przestrzegania w/w Instrukcji.

§3. Wykonanie Zarządzenia powierza się Panu Sławomirowi Sowińskiemu

§4. Zarządzenie wchodzi w życie z dniem podpisania.

§5. Traci moc zarządzenie nr 77/2004 Burmistrza Urzędu Miejskiego w Sulejowie z dnia 10 grudnia 2004 r.

NIE BUDZI ZASTRZEŻEŃ
POD WZGLĘDEM
FORMALNO - PRAWNYM
RADCA PRAWNY
mgr Piotr Organka

BURMISTRZ
Stanisław Baryła

Załącznik Nr 1
do Zarządzenia Nr 78/2012
Burmistrza Sulejowa
z dnia 10 lipca 2012 r.

INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W URZĘDZIE MIEJSKIM W SULEJOWIE UL. KONECKA 42

Sulejów, 10 lipiec 2012 r.

§1

1. Na podstawie art. 36 ust. 1 i 3 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.), §3 ust.3. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U z 2004 r. Nr 100, poz. 1024), ustala się Instrukcję zarządzania systemem informatycznym do przetwarzania danych osobowych w Urzędzie Miejskim w Sulejowie.

2. Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w szczególności:

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, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,
7) sposób realizacji wymogów, o których mowa w §7 ust. 1 pkt 4,
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§2

Przez użyte w Instrukcji określenia należy rozumieć:

- Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 Nr 101, poz. 926 z późn. zm.), osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

- Przetwarzanie danych - jakiekolwiek operacje wykonywane z wykorzystaniem danych, w tym danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

- Zbiór danych osobowych – posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

- **Administrator danych osobowych** – (zwany w skrócie ADO) organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych w jednostce,
- **Administrator bezpieczeństwa informacji** (zwany w skrócie ABI) – osoba lub grupa osób odpowiedzialna za nadzór nad bezpieczeństwem systemów informatycznych i danych osobowych, pełniąca funkcje koordynujące, wykonawcze i kontrolne w tym zakresie.
- **System informatyczny** (zwany w skrócie IT) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Konto** – unikatowy, jednoznacznie identyfikujący użytkownika zasób w systemie informatycznym.
- **Identyfikator użytkownika** – ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- **Hasło** – znany jedynie osobie uprawnionej, ciąg znaków warunkujący dostęp do określonego zasobu w systemie informatycznym,
- **Blokowanie konta** – programowe zablokowanie możliwości korzystania z konta w danym systemie informatycznym.
- **Szkodliwe oprogramowanie** - program komputerowy (kod programu), który może dokonywać niepożądanych zmian w systemie, łącznie z trwałym uszkodzeniem danych lub poważnym zakłóceniem pracy całego systemu.

I. Określenie procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (§5 pkt 1 rozporządzenia)

1. Systemy informatyczne w Urzędzie Miejskim w Sulejowie, w których przetwarzane są dane osobowe, wyposażone są w mechanizmy uwierzytelnienia pracownika, mającego dostęp do tych danych.
2. Dostęp do danych ma pracownik Urzędzie Miejskim w Sulejowie zwany dalej użytkownikiem, spełniający niżej wymienione warunki:
    1) posiada upoważnienie ADO, dopuszczające w zakresie w nim wskazanym, do przetwarzania danych osobowych w systemach informatycznych,
    2) zobowiązuje się do dbałości o bezpieczeństwo danych, do których posiada dostęp, zgodnie z podpisanym oświadczeniem.
3. Pisemny wniosek o zarejestrowanie użytkownika w systemie informatycznym, nadanie, zmianę, bądź usunięcie uprawnień dla pracownika (użytkownika), składa kierownik komórki organizacyjnej lub równorzędny pracownik, do ADO.
4. Wniosek, po zatwierdzeniu przez ADO, zostaje przekazany do ABI, który dokonuje implementacji uprawnień w systemach informatycznych, zgodnie z otrzymanym wnioskiem.
5. Postanowienie to stosuje się odpowiednio w przypadku przejścia pracownika do innej komórki organizacyjnej. Wzór wniosku stanowi Załącznik nr 1 do niniejszej Instrukcji.
6. ABI ustala dla użytkownika odrębny, niepowtarzalny identyfikator, który wprowadzany jest do systemu informatycznego. Użytkownik ustanawia własne hasło podczas pierwszego logowania.

7. Uprawnienia nadane są zgodnie z treścią upoważnienia.
8. Poziom nadawania uprawnień do danych, funkcji i raportów jest rozbudowany o zastosowanie ról systemowych oraz profili bezpieczeństwa.
9. W każdym module systemu zdefiniowane są szczegółowo realizowane funkcjonalności, przy ich udziale można nadać lub odebrać prawo użytkownikowi.
10. Uprawnienia użytkowników rejestrowane są w ewidencji osób zatrudnionych w Urzędzie Miejskim w Sulejowie przy przetwarzaniu danych osobowych oraz w obsługiwanych systemach informatycznych.
11. Modyfikacji uprawnień, lub usunięcia uprawnień użytkownika, dokonuje ABI na podstawie cofnięcia upoważnienia.
12. Wyrejestrowanie użytkownika z dostępu do systemu informatycznego jest równoznaczne z pozbawieniem go praw dostępu do zasobów komputerowych lub sieciowych poprzez zablokowanie konta. Identyfikator użytkownika, który stracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
13. Systemy informatyczne stosowane w Urzędzie Miejskim w Sulejowie wyposażone są w dostępne dla ABI rejestry identyfikujące działania użytkowników.
14. Osobą odpowiedzialną za stosowanie procedur nadania uprawnień i ich rejestrowania w systemie informatycznym jest Administrator Bezpieczeństwa Informacji.
15. ABI może samodzielnie podejmować decyzje o zablokowaniu konta w sytuacjach zagrożenia bezpieczeństwa systemów informatycznych. ABI informuje o powyższym ADO.

II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem (§5 pkt 2 rozporządzenia)

1. Dostęp do programów możliwy jest tylko i wyłącznie po podaniu identyfikatora i hasła.
2. Stosowanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.
3. Identyfikator przydzielany jest indywidualnie dla każdego z użytkowników (hasło zakłada użytkownik).
4. Przydzielone hasło jest zapisywane w systemie w postaci niejawnej.
5. Hasło utrzymywane jest przez użytkownika w tajemnicy, również po upływie ważności.
6. Hasła nie mogą się powtarzać, nie mogą składać się z kombinacji znaków mogących ułatwić odszyfrowanie ich przez osoby nieupoważnione np. imię i nazwisko, nr pokoju, itp.
7. Hasło powinno być zmienione przez użytkownika niezwłocznie w przypadku stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie.
8. Zabronione jest przekazywanie haseł osobom trzecim, w tym również za pośrednictwem niechronionych wiadomości poczty elektronicznej.
9. Za zmianę hasła odpowiedzialny jest użytkownik.
10. Każdy użytkownik zobowiązał się do zachowania tajemnicy w podpisanym oświadczeniu.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu (§5 pkt 3 rozporządzenia)

1. Użytkownik przed przystąpieniem do pracy w systemie informatycznym, zobowiązany jest sprawdzić stanowisko komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych, użytkownik niezwłocznie powiadamia ABI.

2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   a) włączenia komputera,
   b) zalogowania do systemu za pomocą identyfikatora i hasła.

3. Niedopuszczalne jest uwierzytelnianie się poprzez identyfikator i hasło innego użytkownika lub praca w systemie informatycznym na koncie innego, wcześniej zalogowanego użytkownika.
4. Uwierzytelnienie równoznaczne jest z udostępnieniem użytkownikowi zasobów systemu, zgodnie z przydzielonymi uprawnieniami.
5. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności nośniki tj. dyskietki, płyty, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
6. **Niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyciągnięcie wtyczki z kontaktu, bądź pozostawienie włączonych zasobów systemu informatycznego (komputer) po zakończeniu dnia pracy bez nadzoru osób upoważnionych do tych zasobów**.
7. Opuszczając stanowisko pracy użytkownik zamyka szafy i pomieszczenia, w których przechowuje dokumentację i nośniki informacji.
8. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się", zablokować komputer lub zaktywować wygaszacz ekranu z opcją ponownego „logowania" się do systemu.

IV. Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania (§5 pkt 4 rozporządzenia)

1. Użytkownik komputera odpowiedzialny jest za archiwizację, czyli tworzenie kopii bezpieczeństwa zasobów lokalnych.
2. Archiwizowane winny być wszystkie służbowe dokumenty oraz dane, które mają wpływ na funkcjonowanie Urzędu.
3. Użytkownicy lokalnych komputerów zobowiązani są do wykonywania kopii w ciągu ostatniej godziny pracy, tj. umieszczenia aktualnych informacji na nośniku magnetycznym (np. CD-ROM, dodatkowy HDD) lub w udostępnionym folderze.
4. W przypadku wykonywania kopii bezpieczeństwa na nośniku CD-ROM, użytkownik opisuje niezmywalnym markerem płytę CD-ROM (data wykonania kopii bezpieczeństwa, nazwa zbiorów np. *.doc, nazwisko i imię użytkownika, nr inw. stanowiska komputerowego).
5. ABI lub informatyk zobowiązani są do kopiowania danych z dysków sieciowych serwera.

6. Raz na kwartał kopie zapasowe sprawdzane są pod kątem dalszej przydatności do odtworzenia danych na wypadek awarii systemu informatycznego.
7. Kopie zapasowe przechowywane są w innych pomieszczeniach, niż zbiory danych osobowych eksploatowane na bieżąco.
8. Kopiowanie danych osobowych na nośniki informacji w innym celu, niż tworzenie kopii zapasowych jest zabronione. Możliwe tylko w uzasadnionych przypadkach pod warunkiem, że jest to zgodne z przepisami prawa lub na polecenie Burmistrza lub Sekretarza Miasta.
9. Kopie zapasowe po ustaniu ich użyteczności są bezzwłocznie usuwane poprzez nieodwracalne zniszczenie nośnika magnetycznego.

V. Sposób, miejsce i okres przechowywania:

1) **elektronicznych nośników informacji zawierających dane osobowe,**
2) **kopii zapasowych, o których mowa w § 5 pkt 4 rozporządzenia.**

1. Nośniki z danymi osobowymi przechowuje się w miejscach i warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym oraz w sposób uniemożliwiający nieupoważnionym osobom zabranie, zniszczenie lub uszkodzenie tych nośników. Kopie zapasowe przechowywane są w kasie pancernej, w innym pomieszczeniu (bez okien), niż zbiory danych osobowych eksploatowane na bieżąco.
2. Nośniki informacji, które były wykorzystywane do przetwarzania danych osobowych, nie mogą być, bez stosownego zabezpieczenia, przenoszone poza teren Urzędu lub bez ostatecznego usunięcia tych danych, tzn. w sposób uniemożliwiający ich późniejsze odtworzenie.
3. Uszkodzone dyski twarde, dyskietki, taśmy do streamerów i płyty CD, DVD oraz inne nośniki informacji, których dalsza eksploatacja jest niemożliwa, należy zniszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji.
4. Elektroniczne nośniki informacji kopii zapasowych z danymi osobowymi są oznaczane i przechowywane w odpowiednio zabezpieczonych pomieszczeniach, do których dostęp mają wyłącznie upoważnieni pracownicy Urzędu.
5. Wydruki z danymi osobowymi, które nie będą dalej używane, należy zniszczyć w niszczarce.
6. Elektroniczne nośniki informacji przechowuje się w szafach, meblach biurowych niedostępnych dla osób trzecich.
7. Szafy i meble biurowe wykorzystywane m.in. do przechowywania nośników informacji, wyposażone są w co najmniej jeden zamek, a po zakończeniu pracy zamykane.
8. Okres przechowywania kopii zapasowych wynika z trwałości stosowanych nośników magnetycznych lub optycznych.
9. Serwer znajduje się w pomieszczeniu zamykanym, plombowanym po godzinach pracy, niedostępnym dla osób trzecich.
10. Wszystkie pomieszczenia biurowe w Urzędzie Miejskim posiadają drzwi zaopatrzone w zamek, niektóre okna wyposażone są w kraty.
11. Siedziba Urzędu Miejskiego znajduje się w budynku dozorowanym całodobowo.
12. Podstawą przebywania pracownika na terenie budynku poza godzinami pracy jest zgoda bezpośredniego przełożonego.

13. Pobranie i zdanie kluczy reguluje Instrukcja w sprawie wprowadzenia sposobu zabezpieczenia obiektów i pomieszczeń oraz postępowania z kluczami w Urzędzie Miejskim.

VI. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia)

1. Sprawdzanie obecności wirusów komputerowych dokonywane jest przez użytkowników za pomocą programu antywirusowego. Program antywirusowy zainstalowany jest na wszystkich komputerach w Urzędzie Miejskim.
2. Aktualizacja oprogramowania antywirusowego na stanowiskach komputerowych odbywa się automatycznie.
3. Informatyk sprawdza zasoby sieciowe zainstalowane na serwerze pod kątem obecności wirusów, natomiast użytkownicy sprawdzają samodzielnie zasoby lokalne komputera. W przypadku stwierdzenia obecności programów szkodliwych użytkownik niezwłocznie informuje o powyższym ABI i usuwa je przy pomocy zainstalowanego oprogramowania antywirusowego.
4. Po każdej naprawie i konserwacji komputera, należy dokonać sprawdzenia pod kątem występowania oprogramowania szkodliwego i ponownie zainstalować program antywirusowy.
5. Elektroniczne nośniki informacji pochodzenia zewnętrznego oraz dane uzyskiwane drogą teletransmisji (np. pobierane z Internetu) podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.
6. Użytkownicy systemu informatycznego nie są uprawnieni do instalacji jakiegokolwiek oprogramowania. Oprogramowanie na komputerach może być zainstalowane wyłącznie przez informatyka, zgodne z wykazem oprogramowania zainstalowanego na danym komputerze.

VII. Sposób realizacji wymogów, o których mowa w §7 ust. 1 pkt 4 rozporządzenia

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia odnotowanie informacji o udostępnieniach jej danych odbiorcom, w rozumieniu art. 7 pkt 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2002 r. Nr 101 poz. 926 ze zmianami).

VIII. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§5 pkt 8 rozporządzenia)

1. Przeglądy i konserwacja systemu wykonywane są przez informatyka, w przypadku awarii wymagającej interwencji specjalistycznej firmy przez osoby z zewnątrz, pod nadzorem informatyka lub ABI.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych firm zewnętrznych, pozbawia się przed naprawą zapisu tych danych, bądź naprawia się je pod nadzorem osoby upoważnionej – informatyka lub ABI.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie – Załącznik Nr 2 do niniejszej Instrukcji.

4. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.

Załącznik Nr 1
do Instrukcji zarządzania
systemem informatycznym
służącym do przetwarzania
danych osobowych
w Urzędzie Miejskim w Sulejowie

WNIOSEK
O ZAŁOŻENIE UŻYTKOWNIKA /NADANIE UPRAWNIEŃ/MODYFIKACJĘ UPRAWNIEŃ*
DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM
W URZĘDZIE MIEJSKIM W SULEJOWIE

Dane użytkownika:

Nazwisko	
Imię	
Stanowisko służbowe	
Nr upoważnienia do obsługi systemu informatycznego w zakresie przetwarzania danych osobowych	
Login użytkownika w systemie	

Wnioskowane uprawnienia do …….
(nazwa bazy danych)

NAZWA BAZY	Funkcja Administratora	Pełne uprawnienia	Przeglądanie danych
……			

Oświadczam, że zostałam przeszkolona z zasad bezpieczeństwa przetwarzania danych osobowych i zobowiązuję się do ich przestrzegania.	Data, podpis użytkownika profilu
Upoważniam w/w pracownika do obsługi systemu informatycznego w zakresie przetwarzania danych osobowych, zgodnie z ustawą o ochronie danych osobowych z dnia 29-08-1997 r. (Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm.)	Data, podpis Administratora Danych Osobowych

Nadanie/ modyfikację uprawnień wykonał/a:

Nazwisko i imię: _____ / /

Data

Podpis: _____

* niepotrzebne skreślić

Załącznik Nr 2
do Instrukcji zarządzania
systemem informatycznym
służącym do przetwarzania
danych osobowych
w Urzędzie Miejskim w Sulejowie

…… ……
pieczęć nagłówkowa miejscowość, data

PROTOKÓŁ ZNISZCZENIA

KOPII BEZPIECZEŃSTWA*/ INNYCH NOŚNIKÓW ZAWIERAJĄCYCH DANE OSOBOWE*

Nr: .....

Komisja w składzie:

1. .....
2. .....
3. .....

(imię, nazwisko, stanowisko)

oświadcza, iż kopie bezpieczeństwa* / inne nośniki* otrzymane .....
(nazwa komórki organizacyjnej)
zostały w dniu ..... komisyjnie zniszczone.....

.....
(opis procesu zniszczenia)

Rodzaj i oznaczenie nośników:
.....

Ilość (szt.): .....

Uwagi:
.....
.....
.....
.....

Podpisy komisji:

1. .....
2. .....
3. .....

* niepotrzebne skreślić

Załącznik Nr 2
do Zarządzenia Nr 78/2012
Burmistrza Sulejowa
z dnia 10 lipca 2012 r.

POLITYKA BEZPIECZEŃSTWA

W URZĘDZIE MIEJSKIM W SULEJOWIE UL. KONECKA 42

Sulejów, 10 lipiec 2012 r.

Bezpieczeństwo informacji polega na jej ochronie przed przypadkowym lub umyślnym zniszczeniem, ujawnieniem lub modyfikacją.

Polityka Bezpieczeństwa jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu informacji. Dotyczy ona całego procesu korzystania z informacji, niezależnie od sposobu jej gromadzenia i przetwarzania.

1. Polityka bezpieczeństwa w Urzędzie Miejskim w Sulejowie opracowana została, zgodnie z wymogami określonymi w §3 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100 poz. 1024).
2. Polityka bezpieczeństwa w Urzędzie Miejskim w Sulejowie zawiera zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych.
3. Zgodnie z art. 36 ust. 2 oraz art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2002 r. Nr 101 poz. 926, ze zm.), Polityka bezpieczeństwa odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.
4. Celem Polityki bezpieczeństwa jest ustalenie zasad i reguł postępowania w zakresie zabezpieczenia danych osobowych przetwarzanych w Urzędzie Miejskim w Sulejowie.

Procedury zabezpieczania obejmują systemy klasyczne (papierowe) oraz systemy komputerowe.

Gromadzone zasoby narażone są na:

- przechwycenie informacji – naruszenie poufności,
- modyfikację informacji – naruszenie integralności,
- blokowanie dostępu do informacji, zniszczenie informacji – naruszenie dostępności.

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
2) **Przetwarzanie danych** - jakiekolwiek operacje wykonywane z wykorzystaniem danych, w tym danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
3) **Zbiór danych osobowych** – posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
4) **Dane w formie papierowej** – wszelkiego rodzaju dane osobowe przetwarzane i przechowywane w postaci pisemnej.
5) **Administrator danych osobowych** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych w jednostce.
6) **Administrator bezpieczeństwa informacji** (zwany w skrócie ABI) – osoba lub grupa osób odpowiedzialna za nadzór nad bezpieczeństwem systemów informatycznych i danych osobowych, pełniąca funkcje koordynujące, wykonawcze i kontrolne w tym zakresie.
7) **Administrator systemu informatycznego** (zwany w skrócie ASI) – osoba lub grupa osób zarządzająca pracą i zasobami systemów operacyjnych na stacjach klienckich oraz serwerami sieciowymi (administrator sieci), serwerami baz danych, usług i programów.
8) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
9) **Integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
10) **Poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
11) **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

12) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

14) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

15) **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

I. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Urząd Miejski w Sulejowie ma swoją siedzibę w budynku przy ul. Koneckiej 42.

Do obszaru przetwarzania danych osobowych należy zaliczyć wszystkie pomieszczenia będące w posiadaniu Urzędu Miejskiego:

- Wejście A – parter , pokój Nr 1 – Urząd Stanu Cywilnego,
- Wejście A – parter , pokój Nr 2 – Referat Spraw Obywatelskich i Obronnych,
- Wejście A – I piętro , pokój Nr 6 – Referat Organizacyjny,
- Wejście B – parter, pokój Nr 10 – Referat Spraw Obywatelskich i Obronnych,
- Wejście B – I piętro, pokój Nr 13 – Referat Promocji, Kultury, Turystyki, Sportu i Informatyki,
- Wejście B – I piętro, pokój Nr 12 – Stanowisko ds. Sportu, Współpracy, Informatyki
- Wejście C – parter, pokój Nr 14 – Referat Finansów, Podatków i Opłat,
- Wejście C – I piętro, pokój Nr 15, 16, 17, 19 – Referat Infrastruktury i Rozwoju ,
- Wejście C – I piętro, pokój Nr 19a – Referat Gospodarki Ziemią i Rolnictwa,
- Wejście C – I piętro, pokój Nr 18 – Stanowisko ds. Zamówień Publicznych,
- Wejście D – parter, pokój Nr 20, 21, 22, 23, 24 – Referat Finansów, Podatków i Opłat.

II. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

W Urzędzie Miejskim w Sulejowie przetwarza się zbiory danych osobowych przy udziale wymienionych poniżej programów:

1. **„Ewidencja Ludności – miasto i gmina”** (BDF_EUM) – Firma P.T.H. „BDF-elin” Sp. z o.o., Bełchatów, ul. Wyspiańskiego 4.

2. **Podatki i opłaty lokalne dla gminy i miasta** (BDF_Podatki.net) - „BDF-elin” Sp. z o.o., Bełchatów, ul. Wyspiańskiego 4.

3. **Programy finansowo-księgowe** (BDF_FKG) - Firma „BDF-ELIN” Sp. z o.o., Bełchatów, ul. Wyspiańskiego 4.

4. Program **„Ewidencja gruntów i budynków” (EGB)** – realizuje komputerową obsługę bazy danych ewidencji gruntów i budynków w zakresie treści obligatoryjnej – przeglądanie danych. Dane pozyskiwane są przez Urząd Miejski w Sulejowie od właściwej jednostki - Starostwa Powiatowego w Piotrkowie Trybunalskim prowadzącego przedmiotową ewidencję.

5. **System PB_USC – Firmy** TECHNIKA IT S.A. **ul. Toszecka 244-102 Gliwice, wspiera rejestrację aktów stanu cywilnego, zgodnie z obowiązującą ustawą i aktami wykonawczymi do niej.**

6. **System „Płatnik” –** system służący do rozliczeń pracowników z ZUS.

7. ePFRON

Programy:

1. „Ewidencja Ludności”,
2. Podatki i opłaty lokalne dla gminy i miasta,
3. Programy finansowo-księgowe, zainstalowane są na serwerze.
   Parametry serwera: Procesor 2 x Quad-Core Xeon E5345 2.33Ghz, Pamięć 4GB (2 x 2Gb DIMMs) 667MHz FBD, dyski SAS: 2x150GB + 2x300GB RAID0, system operacyjny

– MS Windows Server 2003, zasilacz awaryjny UPS 1200 VA. Baza Danych Oracle 10g, Pervasive v8.

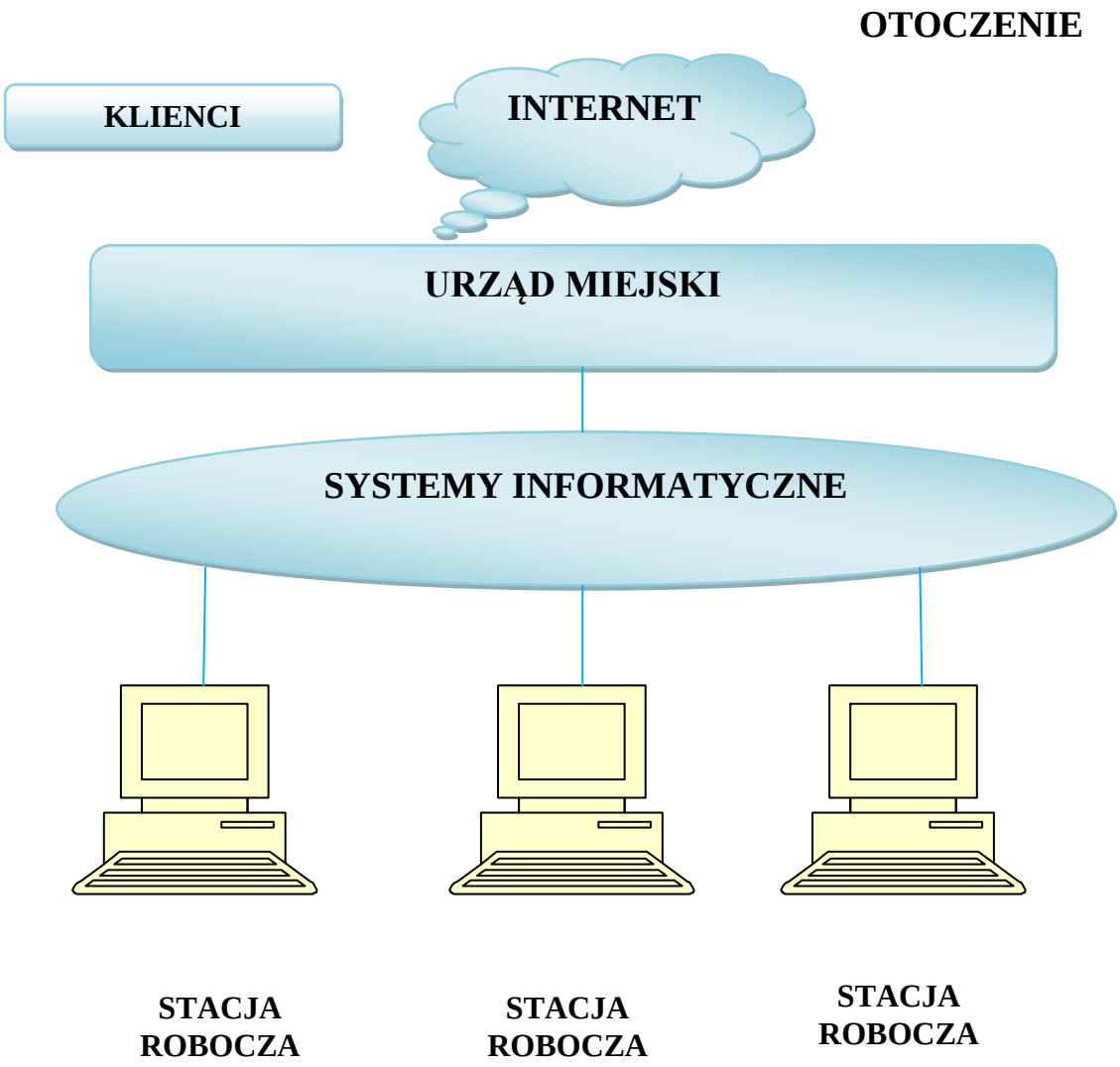
4. **„Ewidencja gruntów i budynków" na stanowisku komputerowym wyposażonym w system operacyjny MS Windows XP Professional** i zasilacz awaryjny UPS Ever 500 Pro, komputer wyposażony jest system antywirusowy ESET Smart Security łączący ochronę antywirusową i antyspyware z zaporą osobistą i modułem antyspamowym wraz z szeregiem nowych, zaawansowanych funkcji bezpieczeństwa.
5. **System PB_USC** stworzony został w oparciu o bazę danych firmy MS SQL, korzysta z jednej integralnej bazy danych, wyposażony jest w system udostępniania i ochrony danych**, system działa na 1 stanowisku komputerowym, wyposażonym w MS Winsows XP Professional i zasilacz awaryjny UPS. K**omputer wyposażony jest system antywirusowy ESET Smart Security łączący ochronę antywirusową i antyspyware z zaporą osobistą i modułem antyspamowym wraz z szeregiem nowych, zaawansowanych funkcji bezpieczeństwa.
6. **PŁATNIK, ePFRON na stanowisku komputerowym wyposażonym w system operacyjny MS Windows XP Professional** i zasilacz awaryjny UPS Ever 500 Pro, komputer wyposażony jest system antywirusowy ESET Smart Security łączący ochronę antywirusową i antyspyware z zaporą osobistą i modułem antyspamowym wraz z szeregiem nowych, zaawansowanych funkcji bezpieczeństwa.

Każdy użytkownik ma określony:

1) Zakres danych, z których może korzystać oraz operacje, jakie może na nich wykonać (uprawnienia do wprowadzania, aktualizacji, akceptacji, przeglądania, wydruków, pełne prawa, itp.)
2) Rolę systemu wspólną dla grupy pracowników realizującej takie samo zadanie (np. kasjerzy, księgowe itp.).
3) Prowadzenie historii wprowadzonych zmian danych w systemie, z rejestracją daty, czasu i osoby wprowadzającej zmiany.

Bazy danych zainstalowane są na serwerze, realizowane są na modelu relacyjnym w standardzie SQL-a. Wielodostęp działa w modelu klient-serwer z kontrolą śledzenia zupełności transakcji. Dostęp do informacji chroniony jest hasłami z selekcją praw do zapisu danych.

III. OPIS STRUKTURY ZBIORÓW WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI



„EWIDENCJA LUDNOŚCI – MIASTO I GMINA” (BDF_EUM).

Zgodnie z obowiązującymi przepisami, wynikającymi z ustawy o ewidencji ludności i dowodach osobistych oraz przepisów wykonawczych do tej ustawy, oraz w myśl realizowanej koncepcji Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), gminy obsługiwane są systemami informatycznymi Lokalnego Banku Danych (LBD). System ewidencji ludności poziomu gminy stanowi najniższe ogniwo w hierarchii systemów

informatycznych PESEL. Wynikają stąd funkcje mające zapewnić pełną kompatybilność oraz ciągłą komunikację informatyczną LBD z systemami wyższych poziomów, a mianowicie:

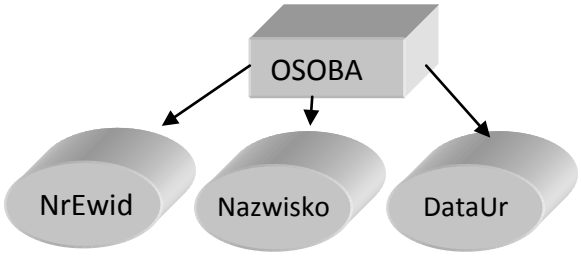
- Terenowym/Wojewódzkim Bankiem Danych (TBD/WBD);
- Rejestrem PESEL-CBD.

Warunkiem dopuszczenia systemu ewidencji ludności LBD do eksploatacji użytkowej jest uzyskanie świadectwa homologacji.

Departament Rozwoju Informatyki i Systemu Rejestrów Państwowych Ministerstwa Spraw Wewnętrznych i Administracji opracował wytyczne dla projektanta – programisty. Wytyczne te ściśle precyzują warunki dotyczące:

- struktury banku danych i rekordu,
- kontroli formalnej i logicznej danych,
- standardów kodowania danych,
- wykonywanych funkcji przetwarzania,
- komunikacji z innymi poziomami systemu PESEL,
- parametrów techniczno-eksploatacyjnych.

Schemat przedstawia podstawowy zakres danych osobowych.



Przedstawiony schemat OSOBA możemy przedstawić także za pomocą tabeli o następującym schemacie:

Osoba(NrEwid, Nazwisko, DataUr)

gdzie NrEwid jest kluczem głównym.

Zakres przedmiotowy rekordu dotyczącego osoby:

Nazwa informacji
Dane identyfikacyjne Numer ewidencyjny PESEL
Data wprowadzenia rekordu
Data ostatniej aktualizacji Nazwisko aktualne – pierwszy człon Nazwisko aktualne – drugi człon Imię aktualne – pierwszy człon
Imię aktualne – drugi człon
Nazwisko rodowe – pierwszy człon Nazwisko rodowe – drugi człon **Dane o urodzeniu** Nazwisko ojca – pierwszy człon Nazwisko ojca – drugi człon Imię ojca – pierwszy człon Imię ojca - drugi człon Nazwisko rodowe ojca - pierwszy człon
Nazwisko rodowe ojca - drugi człon Nazwisko matki – pierwszy człon Nazwisko matki – drugi człon Imię matki – pierwszy człon Imię matki - drugi człon
Nazwisko rodowe matki - pierwszy człon
Nazwisko rodowe matki - drugi człon Miejsce urodzenia USC - rejestracja (kod terytorialny) Numer aktu urodzenia Data wystawienia aktu urodzenia **Nazwiska poprzednie** Nazwisko poprzednie - pierwszy człon Nazwisko poprzednie - drugi człon Data zmiany Numer dokumentu lub sygnatura akt **Imiona poprzednie** Imię poprzednie – pierwszy człon Imię poprzednie – drugi człon Data zmiany
Kod terytorialny + kod organu rej.
Numer akt **Stany cywilne** Kod stanu cywilnego
Data zmiany
Numer akt

Nazwa informacji
Nazwisko współmałżonka - pierwszy człon Nazwisko współmałżonka - drugi człon Imię współmałżonka - pierwszy człon
Imię współmałżonka - drugi człon
Numer ewidencyjny współmałżonka Kod formy ustania małżeństwa **Adres aktualny zameldowania na pobyt stały**
Kod terytorialny
Miejscowość Ulica Numer domu Numer lokalu Kod pocztowy Data zameldowania **Adresy poprzednie zameldowania na pobyt stały** Kod terytorialny Miejscowość
Ulica Numer domu Numer lokalu Kod pocztowy Data zameldowania Data wymeldowania Kod rodzaju wymeldowania **Adresy czasowe - pobyt ponad 2 miesiące** Kod terytorialny
Miejscowość Ulica Numer domu
Numer lokalu Kod pocztowy Data zameldowania Data wymeldowania **Dokumenty tożsamości** Kod rodzaju dokumentu Seria i numer dokumentu Kod terytorialny wystawcy dokumentu Kod wystawcy dokumenty
Data wydania dokumentu
Rysopis
Wzrost

Nazwa informacji
Kod koloru oczu Kod znaku szczególnego **Wojsko** Kod czy podlega
Stopień wojskowy – kod
Kod rodzaju dokumentu wojskowego Seria i numer dokumentu wojskowego **Zgon** Data zgonu
Kod teryt. USC rejestrującego zgon Kod organu
Numer aktu zgonu

W związku z potrzebą zapisu niektórych grup informacji, system utrzymuje odpowiednie zbiory archiwalne. Jak wynika ze struktury rekordu, konieczności zapamiętania informacji archiwalnych podlegają:

- nazwiska poprzednie;
- imiona poprzednie;
- stany cywilne;
- poprzednie adresy stałe;
- poprzednie adresy czasowe;
- poprzednie dokumenty tożsamości;

Przenoszenie danych z rekordu podstawowego do archiwum oraz jego reorganizacja celem zachowania koniecznej chronologii zapisów wykonuje się automatycznie.

Podatki i opłaty lokalne dla gminy i miasta (BDF_Podatki.net**).**

PODATEK OD NIERUCHOMOŚCI

Podstawowym aktem normatywnym, regulującym wymiar i pobór podatku od nieruchomości, jest ustawa o podatkach i opłatach lokalnych. Podatek od nieruchomości należy do grupy tak zwanych podatków lokalnych, stanowiących w całości dochód budżetu gminy.

Podmiotami, na których ciąży obowiązek podatkowy są: osoby fizyczne, osoby prawne, jednostki organizacyjne nie mające os. prawnej, spełniające następujące przesłanki:

- są właścicielami lub samoistnymi posiadaczami nieruchomości albo obiektów budowlanych nie złączonych trwale z gruntem,
- są użytkownikami wieczystymi nieruchomości lub ich części,
- są posiadaczami nieruchomości albo obiektów budowlanych nie złączonych trwale z gruntem, stanowiących własność Skarbu Państwa lub jednostki samorządu terytorialnego, jeżeli posiadanie wynika z umowy zawartej z właścicielem lub innego tytułu prawnego,
- posiadają bez tytułu prawnego nieruchomości lub ich części albo obiekty budowlane nie złączone trwale z gruntem, stanowiące własność Skarbu Państwa lub jednostki samorządu terytorialnego, z wyjątkiem nieruchomości wchodzących w skład Zasobu Własności Rolnej Skarbu Państwa lub będących w zarządzie Lasów Państwowych.

W pierwszej kolejności - gdy znany jest właściciel - obowiązek podatkowy ciąży na właścicielu nieruchomości. W przypadku, gdy nie można ustalić bezspornego i aktualnego stanu prawnego, wynikającego z danych posiadanych przez organ podatkowy (np. w oparciu o ewidencję gruntów) obowiązek podatkowy będzie ciążyć na samoistnym posiadaczu.

Opodatkowaniu podlegają:

- budynki lub ich części,
- budowle lub ich części związane z prowadzeniem działalności gospodarczej innej niż działalność rolnicza lub leśna,
- grunty nie objęte przepisami o podatku rolnym lub leśnym,
- grunty objęte przepisami o podatku rolnym lub leśnym, związane z prowadzeniem działalności gospodarczej innej niż działalność rolnicza lub leśna oraz nie sklasyfikowane grunty.
- grunty pod jeziorami, grunty zajęte na zbiorniki wodne retencyjne lub elektrowni wodnych.

Podstawę opodatkowania stanowią:

- dla budynków lub ich części - powierzchnia użytkowa,
- dla budowli - ich wartość ustalona na dzień 1 stycznia roku podatkowego, stanowiąca podstawę obliczania amortyzacji w tym roku, a w przypadku budowli całkowicie zamortyzowanych - ich wartość z dnia 1 stycznia roku, w którym dokonano ostatniego odpisu amortyzacyjnego,
- dla gruntów - powierzchnia tych gruntów.

Wymiar podatku od nieruchomości jest dokonywany na podstawie danych wynikających z ewidencji gruntów i budynków prowadzonej dla danej miejscowości i do czasu wprowadzenia zmian w ewidencji ujawnione w niej dane są wiążące dla organu podatkowego. Dotyczy to w szczególności takich danych, jak położenie działki, jej granice, rodzaje użytków i ich jakość.

Zgodnie z obowiązującym prawem system informatyczny obsługujący sprawy związane z podatkiem od nieruchomości bazuje na tak zwanej kartotece nieruchomości, zawierającej karty nieruchomości.

Karta nieruchomości zawiera informacje o nieruchomości, o podstawach jej opodatkowania, informacje o podatniku i innych osobach (współwłaścicielach itp.), a w szczególności:

- dokładne dane adresowe nieruchomości,
- dane podatnika,
- dane innych osób związanych z własnością lub użytkowaniem nieruchomości,
- opis tytułów podatkowych,
- informacje o podstawie opodatkowania,
- ulgi i zwolnienia przysługujące w danym roku podatkowym.

Należy zwrócić uwagę, że dany adres nieruchomości może być podany więcej niż jeden raz i każdy z nich może mieć innych współwłaścicieli. Dlatego wymagane jest opatrzenie każdej karty nieruchomości unikalnym numerem.

Dla uzyskania prawidłowej funkcjonalności kartoteki dane osobowe podatnika zawierają następujące informacje:

- nazwisko i imię (imiona)
- adres pobytu stałego,
- ewentualny adres do korespondencji,
- numer ewidencyjny PESEL
- numer identyfikacji podatkowej NIP

PODATEK ROLNY

Podstawowym aktem normatywnym, regulującym wymiar i pobór podatku rolnego, jest ustawa o podatku rolnym.

Podatnikami podatku rolnego są osoby fizyczne, osoby prawne, jednostki organizacyjne, w tym spółki nieposiadające osobowości prawnej, będące:

- właścicielami gruntów,
- posiadaczami samoistnymi gruntów,
- użytkownikami wieczystymi gruntów,
- posiadaczami gruntów stanowiących własność Skarbu Państwa lub jednostki samorządu terytorialnego, jeżeli posiadanie wynika z umowy zawartej z właścicielem lub z innego tytułu prawnego, bądź jest bez tytułu prawnego.

Karta gospodarstwa rolnego zawiera informacje o podstawach opodatkowania, informacje o podatniku i innych osobach (współwłaścicielach itp.), a w szczególności:

- dokładne dane adresowe gospodarstwa,
- dane podatnika,
- dane innych osób związanych z własnością lub użytkowaniem nieruchomości,
- opis tytułów podatkowych,
- informacje o podstawie opodatkowania.

Każda karta gospodarstwa oznaczona jest unikalnym numerem.

Dane dotyczące podatnika zawierają informacje analogiczne do informacji zawartych w karcie nieruchomości.

Opis tytułów podatkowych i informacje o podstawach opodatkowania zawierają następujące informacje:

- typ własności (określający, czy grunty stanowią własność podatnika, czy są wydzierżawiane lub użytkowane na podstawie innego tytułu prawnego)
- numer okręgu podatkowego,
- rodzaj gruntu,
- klasa gruntu,
- powierzchnia (w hektarach fizycznych)
- ulgi i zwolnienia przysługujące w danym roku podatkowym,
- data nabycia,
- data zbycia.

PODATEK LEŚNY

Podstawowym aktem normatywnym, regulującym wymiar i pobór podatku leśnego, jest ustawa o podatku leśnym.

Podatnikami podatku leśnego są osoby fizyczne, osoby prawne, jednostki organizacyjne, w tym spółki nieposiadające osobowości prawnej, będące:

- właścicielami lasów,
- posiadaczami samoistnymi lasów,
- użytkownikami wieczystymi lasów,
- posiadaczami lasów stanowiących własność Skarbu Państwa lub jednostki samorządowej.

Lasem są grunty leśne sklasyfikowane w ewidencji gruntów i budynków (prowadzonej przez starostę) jako lasy.

Karta lasu powinna zawierać informacje o podstawach opodatkowania, informacje o podatniku i innych osobach (współwłaścicielach itp.), a w szczególności:

- dokładne dane adresowe gospodarstwa,
- dane podatnika,
- dane innych osób związanych z własnością lub użytkowaniem nieruchomości,
- opis tytułów podatkowych,
- informacje o podstawie opodatkowania,
- ulgi i zwolnienia przysługujące w danym roku podatkowym.

Opis tytułów podatkowych i informacje o podstawach opodatkowania zawierają następujące informacje:

- typ własności (określający, czy lasy stanowią własność podatnika, czy są wydzierżawiane lub użytkowane na podstawie innego tytułu prawnego)
- powierzchnia wyrażona w hektarach fizycznych,
- data nabycia,
- data zbycia.

IV. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI

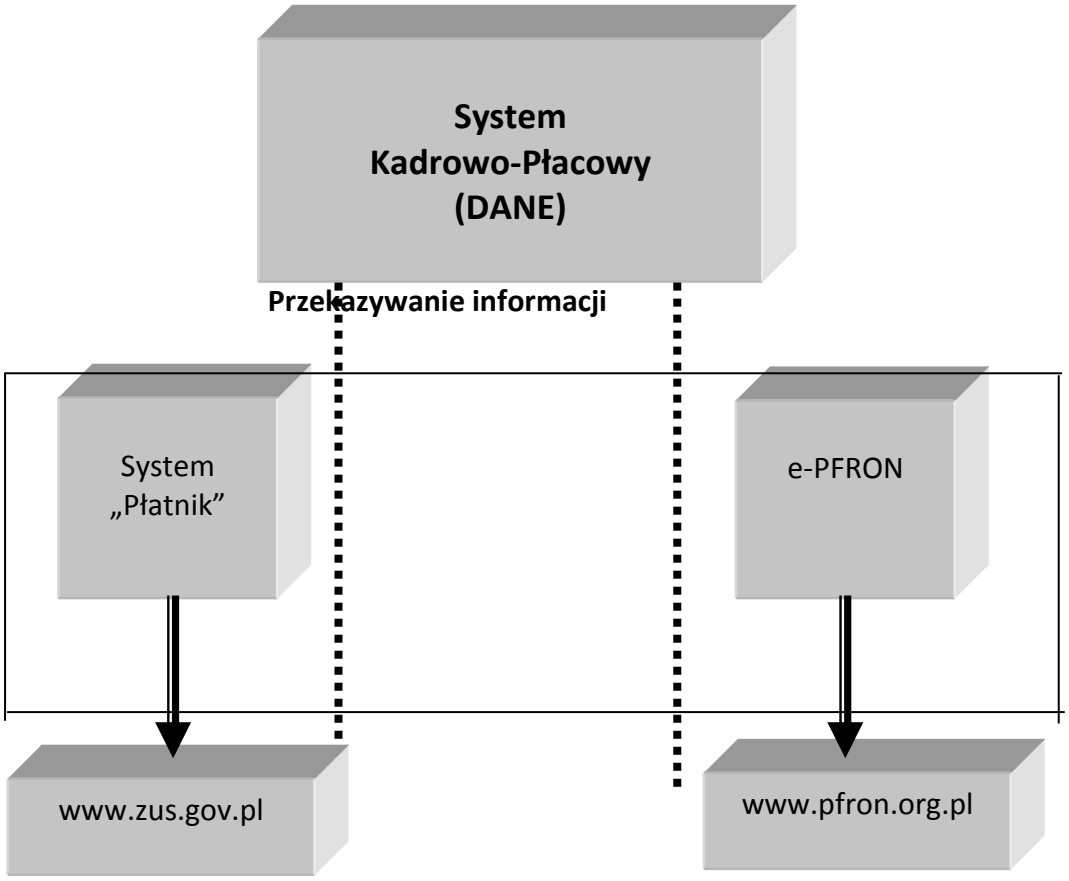
Poniższe schematy przedstawiają współpracę systemów informatycznych eksploatowanych w Urzędzie Miejskim w Sulejowie.
Zainstalowane w Urzędzie Miejskim systemy informatyczne po osiągnięciu pełnej funkcjonalności wszystkich modułów mają zapewnić integrację i kompatybilność danych oraz umożliwić ich wykorzystanie w każdym czasie i wg. potrzeb.

Podstawowym zadaniem ich jest:

1) zapewnienie wysokiej jakości informacji wykorzystywanych w procesach decyzyjnych,
2) kompleksowa funkcjonalność obejmującą obszar działalności finansowo-księgowej,
3) gospodarka zasobami ludzkimi,
4) integracja danych i procesów – dotycząca wymiany danych, zarówno wewnątrz obiektu (między modułami), jak i z jego otoczeniem (np. poprzez elektroniczną wymianę danych).

2. W programie **PŁATNIK** dane ubezpieczeniowe osób zarejestrowanych w systemie są przesyłane poprzez łącze internetowe do jednostki ZUS. Dane te przesyłane są na serwery znajdujące się pod adresami:

- http://www.sdwi.warszawa.zus.pl,
- http://www.sdwi.wrocław.zus.pl,
- http://www.sdwi.gdansk.zus.pl.



Systemy: **„PŁATNIK” I „ePFRON”** zapewniają pełne bezpieczeństwo i poufność przesyłanych danych poprzez:

1) zastosowanie podpisu elektronicznego do weryfikacji autoryzacji dokumentów,
2) wykorzystanie protokołu https (SSL do transmisji danych – szyfrowanie),
3) zabezpieczenie dostępu do kont użytkowników przy pomocy hasła,
4) ograniczenie ilości prób błędnego logowania oraz wykorzystanie uprawnień.

V. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Przetwarzane dane osobowe stanowią zasoby, które wymagają odpowiedniej ochrony przed zagrożeniami w celu zapewnienia ciągłości pracy i minimalizacji strat. Informacja istnieje w wielu postaciach. Może być wydrukowana lub zapisana na papierze, przechowywana elektronicznie, przesyłana pocztą lub za pomocą środków elektronicznych.

Bez względu na postać, którą przybiera informacja oraz środki za pomocą, których jest udostępniana lub przechowywana, zawsze powinna być właściwie chroniona.

Bezpieczeństwo informacji określa się najczęściej jako zachowanie:

1) poufności - zapewnienia, że informacja jest dostępna wyłącznie dla tych, którym zostało przyznane prawo dostępu,
2) integralności - zagwarantowania dokładności i kompletności informacji i metod jej przetwarzania,
3) dostępności - zapewnienia, że uprawnieni użytkownicy mają dostęp do informacji i związanych z nią zasobów, gdy jest to wymagane.

Za naruszenie ochrony systemu informatycznego uważa się w szczególności:

1) nieupoważniony dostęp lub próbę dostępu do danych osobowych,
2) kradzież nośników zawierających dane osobowe,
3) zniszczenie lub próby zniszczenia danych zgromadzonych w systemie,
4) wprowadzenie wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
5) zagrożenia wynikające z technologii używanych przy przetwarzaniu – awarie sprzętowe, awarie systemowe i błędy programowe.

W celu uniemożliwienia dostępu osób trzecich do danych osobowych przetwarzanych w Urzędzie Miejskim w Sulejowie, podjęto stosowne środki techniczne i organizacyjne:

1) zabezpieczenie wejścia do budynków po godzinach pracy.
2) wyposażenie pomieszczeń w szafy zamykane na klucz,
3) zakaz podłączania do sieci elektrycznej (związanej z infrastrukturą informatyczną) urządzeń wysokiej mocy, takich jak: czajniki elektryczne, wentylatory itp.,
4) zapoznanie osób dopuszczonych do pracy przy przetwarzaniu danych osobowych z przepisami ustawy o ochronie danych osobowych,
5) zabezpieczenie dostępu do kluczy do pomieszczenia serwerowni, kasy itp.,
6) w trakcie przetwarzania danych osobowych, pracownik jest odpowiedzialny za bezpieczeństwo powierzonych mu danych,
7) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych należy sprawdzić, czy posiadane dane były należycie zabezpieczone oraz

czy zabezpieczenia te nie były naruszone,

8) w trakcie przetwarzania danych osobowych, należy dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
9) po zakończeniu przetwarzania danych pracownik należycie zabezpiecza dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

W razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego pracownik zobowiązany jest niezwłocznie powiadomić o zaistniałym fakcie ABI.

ABI po otrzymaniu powiadomienia:

1) podejmuje stosowne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu,
2) zabezpiecza, utrwala informacje będące źródłem przy ustaleniu przyczyn naruszenia,
3) dokonuje analizy stanu systemu informatycznego oraz analizy szkód powstałych na skutek naruszenia,
4) sporządza szczegółowy raport zawierający datę i godzinę otrzymania informacji naruszeniu, opis przebiegu, przyczyny oraz wnioski z zaistniałej sytuacji,
5) niezwłocznie przywraca prawidłowy stan działania systemu, w razie potrzeby odtwarza dane z kopii awaryjnych.

Sporządzony raport z kopiami dokumentów (np. kopie dowodów), administrator bezpieczeństwa informacji przekazuje administratorowi danych.

Informatyk/Administrator bezpieczeństwa informacji wraz z Administratorem danych podejmują niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu.

Każda osoba wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zobowiązana jest do zapoznania się i przestrzegania Polityki bezpieczeństwa.

Aplikacje służące do elektronicznego przekazywania dokumentów zapewniają pełne bezpieczeństwo i poufność przesyłanych danych poprzez zastosowanie podpisu elektronicznego, wykorzystanie protokołu https (SSL do transmisji danych – szyfrowanie), zabezpieczenie dostępu do kont użytkowników przy pomocy hasła, ograniczenie ilości prób błędnego logowania oraz wykorzystanie uprawnień.

Systemy działają z dostępem do Internetu, sprzęt zabezpieczony jest koniecznością podania identyfikatora użytkownika i hasła w momencie logowania, na komputerach zainstalowano system antywirusowy na bieżąco aktualizowany, zainstalowano firewall.

W ramach zabezpieczenia danych osobowych ochronie podlegają:

1) sprzęt komputerowy – serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne,
2) oprogramowanie – kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne,
3) dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie,
4) hasła użytkowników,
5) kopie zapasowe i archiwa,
6) dokumentacja – zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje, itp.,
7) wydruki.

Pracownicy zatrudnieni w Urzędzie Miejskim zobowiązani są stosować środki techniczne i organizacyjne zapewniające ochronę adekwatną do zagrożeń.
Odpowiadają za bezpieczeństwo i za prawidłową eksploatację systemu informatycznego na użytkowanym komputerze.

W przypadku korzystania z komputera przez kilku użytkowników kierownicy komórek organizacyjnych, wyznaczają osobę odpowiedzialną za sprzęt.

Użytkownicy systemów komputerowych mają obowiązek postępowania zgodnie z Instrukcją określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych oraz Polityką bezpieczeństwa.

§13

Dane osobowe, przetwarzane w Urzędzie Miejskim, mogą być udostępniane wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania. Dane osobowe udostępnia się na pisemny, umotywowany wniosek chyba, że przepis innej ustawy stanowi inaczej. Wniosek, o którym mowa powyżej, powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazać ich zakres i przeznaczenie. Wzór wniosku o udostępnienie danych ze zbioru danych osobowych określają przepisy powszechnie obowiązujące.

§14

WYKAZ ZAŁĄCZNIKÓW DO POLITYKI BEZPIECZEŃSTWA

Załącznik Nr 1	Wzór upoważnienia dopuszczającego do przetwarzania danych osobowych w Urzędzie Miejskim w Sulejowie
Załącznik Nr 2	Wzór oświadczenia o zapoznaniu się z przepisami obowiązującymi przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Sulejowie
Załącznik Nr 3	Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Sulejowie
Załącznik Nr 4	Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych w Urzędzie Miejskim w Sulejowie
Załącznik Nr 5	Obszar przetwarzania danych osobowych w Urzędzie Miejskim w Sulejowie
Załącznik Nr 6	Wykaz zbiorów zawierających dane osobowe przetwarzane w Urzędzie Miejskim w Sulejowie
Załącznik Nr 7	Analiza ryzyka występującego przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Sulejowie
Załącznik Nr 8	Opis struktury zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Sulejowie wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Załącznik Nr 1
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

Sulejów, dn. .....

UPOWAŻNIENIE DOPUSZCZAJĄCE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr ……. / ROK

Burmistrz Sulejowa działając na podstawie art. 37 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. Nr 133, poz. 883 ze zmianami) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), upoważnia Panią/Pana*

……

(imię i nazwisko)

……

(nazwa stanowiska)

do przetwarzania danych osobowych w systemie informatycznym, w kartotekach, skorowidzach, księgach, wykazach, z zakresu:

……

(nazwa przetwarzanych danych osobowych)

……

(nazwa przetwarzanych danych osobowych)

oraz urządzeń wchodzących w jego skład.

Upoważnienie wygasa z chwilą ustania Pani/Pana zatrudnienia w Urzędzie Miejskim w Sulejowie.

....
Administrator Danych Osobowych data i podpis osoby upoważnianej

* niepotrzebne skreślić

Załącznik Nr 2
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

Piotrków Trybunalski, dnia ..... 2012 r.

NAZWISKO I IMIĘ: ……

NAZWA KOMÓRKI ORGANIZACYJNEJ ……

OŚWIADCZENIE
W SPRAWIE ZAZNAJOMIENIA Z PRZEPISAMI DOTYCZĄCYMI OCHRONY DANYCH OSOBOWYCH

Ja niżej podpisana/y, zatrudniona/y w Urzędzie Miejskim w Sulejowie, ul. Konecka 42, na stanowisku ....., wiążącym się z wykonywaniem pracy przy przetwarzaniu danych osobowych oświadczam, że zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024) zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, a w szczególności z:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2004 r. Nr 101, poz. 926 z późn. zmianami),
2) rozporządzeniem z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024),
3) Polityką bezpieczeństwa wprowadzoną Zarządzeniem Nr ……. Burmistrza Sulejowa z dnia …… 2012 r.,
4) Instrukcją określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, wprowadzoną Zarządzeniem Nr ……. Burmistrza Sulejowa z dnia …….. 2012 r.,
5) Instrukcją określającą prawa i obowiązki użytkowników sprzętu komputerowego służącego do przetwarzania danych osobowych w Urzędzie Miejskim w Sulejowie , wprowadzoną Zarządzeniem Nr ……. Burmistrza Sulejowa z dnia …… 2012 r.,
6) Instrukcją w sprawie zasad postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Sulejowie , wprowadzoną Zarządzeniem Nr ……. Burmistrza Sulejowa z dnia …….. 2012 r.,
7) Ponadto pracując na sprzęcie komputerowym o nr inw. …… zobowiązuję się:

1. Dbać o bezpieczeństwo wszystkich danych, do których posiadam dostęp, w szczególności do danych na dysku lokalnym, danych w sieci komputerowej, jak i danych na nośnikach magnetycznych (zewnętrznych) – optycznych, pendrive.
2. Systematycznie wykonywać kopie zapasowe danych gromadzonych na dysku lokalnym powierzonego komputera.
3. Sprawdzać przy pomocy programu antywirusowego, czy dane gromadzone na dysku lokalnym powierzonego komputera oraz dane pochodzące ze źródeł zewnętrznych (dyskietki, płyty CD, internet) nie zawierają wirusów komputerowych.
4. Przestrzegać przepisów o prawie autorskim w części dotyczącej programów komputerowych do pracy tylko na programach oficjalnie zakupionych przez Urząd Miejski w Sulejowie - nie instalowania programów pochodzących z innych źródeł, nie udostępniania programów będących własnością Urzędu Miejskiego w Sulejowie osobom trzecim.
5. Prawidłowo obsługiwać powierzony mi sprzęt komputerowy, chronić go przed fizycznym uszkodzeniem (zalanie, zrzucenie itp.) oraz utrzymywać sprzęt w czystości.

6. Nie zmieniać konfiguracji w powierzonym sprzęcie.

7. Jednocześnie zobowiązuje się do zachowania w tajemnicy danych osobowych, które przetwarzam w czasie zatrudnienia w Urzędzie Miejskim oraz po jego ustaniu.

Naruszenie powyższych zobowiązań skutkuje odpowiedzialnością cywilną i karną wynikającą z:

1. przepisów z dnia 29 sierpnia 1997 r., rozdział 8 ustawy o ochronie danych osobowych (Dz.U. z 2004 r. Nr 101, poz. 926 z późn. zmianami),
2. rozdziału 9 i 14 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2000 r. Nr 80, poz. 904 z późn. zmianami).

.....
(data i czytelny podpis pracownika)

Załącznik Nr 3
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

Piotrków Tryb., dn. .....

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Sulejowie

LP.	NAZWA MODUŁU ZSI/NAZWA PROGRAMU	NAZWISKO I IMIĘ UŻYTKOWNIKA	NR UPOWAŻNIENIA	DATA ZAREJESTROWANIA	DATA WYREJESTROWANIA	UWAGI

Załącznik Nr 4
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

Piotrków Tryb., dn. .....

Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych zainstalowanych na serwerze w Urzędzie Miejskim w Sulejowie

Lp.	Nazwa bazy danych	Nazwisko i imię użytkownika	Identyfikator w systemie informatycznym	Rodzaj uprawnień*	Uwagi
1					
2					
3					

* Skróty stosowane do określenia uprawnień:
1) Funkcja Administratora - FA
2) Pełne uprawnienia - PU
3) Przeglądanie - PR

Załącznik Nr 5
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

Obszar przetwarzania danych osobowych
w Urzędzie Miejskim w Sulejowie

1. Zbiory danych przetwarzane w systemach informatycznych:

Lp.	Pomieszczenie	Bazy danych przetwarzane lokalnie	Dostęp do baz danych przetwarzanych sieciowo

2. Zbiory danych przetwarzane w postaci dokumentacji papierowej:

Lp.	Pomieszczenie	Dokumentacja papierowa - Kartoteki

Załącznik Nr 6
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

Piotrków Trybunalski, dnia …….

INWENTARYZACJA ZBIORÓW DANYCH OSOBOWYCH
PRZEPROWADZONA W URZĘDZIE MIEJSKIM W SULEJOWIE

Lp.	Nazwa zbioru	Wykorzystanie systemu informatycznego		Przetwarzanie „systemem papierowym”	Uwagi
		Nazwa aplikacji	Nazwa i Adres Firmy	Określenie miejsca przechowywania dokumentów	

Załącznik Nr 7
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

ANALIZA RYZYKA
WYSTĘPUJĄCEGO PRZY PRZETWARZANIU ZBIORÓW DANYCH OSOBOWYCH
W URZĘDZIE MIEJSKIM W SULEJOWIE

§1

Analiza ryzyka dla dokumentacji papierowej

Rodzaj zagrożenia	Prawdopodobieństwo	Koszt	Uwagi

§2

Analiza ryzyka dla baz danych przetwarzanych w systemie informatycznym

Rodzaj zagrożenia	Prawdopodobieństwo	Koszt	Uwagi

Załącznik Nr 8
do Polityki bezpieczeństwa
w Urzędzie Miejskim w Sulejowie

OPIS
STRUKTURY ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH
W URZĘDZIE MIEJSKIM W SULEJOWIE

Załącznik Nr 3
do Zarządzenia Nr 78/2012
Burmistrza Sulejowa
z dnia 10 lipca 2012 r.

INSTRUKCJA
OKREŚLAJĄCA PRAWA I OBOWIĄZKI UŻYTKOWNIKÓW SPRZĘTU KOMPUTEROWEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W SULEJOWIE

§1

1. Użytkownik sprzętu komputerowego ma prawo do korzystania wyłącznie w celach służbowych i na zasadach określonych w niniejszej instrukcji z:
   1) zasobów lokalnych tworzonych na dysku twardym komputera,
   2) zasobów sieciowych udostępnionych przez indywidualne konto użytkownika, zgodnie z dokumentem „Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Sulejowie”,
   3) drukarek lokalnych i sieciowych,
   4) oprogramowania określonego w wykazie oprogramowania zainstalowanego na danym komputerze.
   5) usług sieci Internet.

2. Obowiązkiem użytkownika sprzętu komputerowego jest:
   1) dbać o bezpieczeństwo wszystkich danych, do których posiada dostęp, w szczególności do danych na dysku lokalnym, danych w sieci komputerowej, jak i danych na nośnikach zewnętrznych – optycznych, flash,
   2) systematycznie wykonywać kopie zapasowe danych gromadzonych na dysku lokalnym powierzonego komputera,
   3) sprawdzać przy pomocy programu antywirusowego, czy dane gromadzone na dysku lokalnym powierzonego komputera oraz dane pochodzące ze źródeł zewnętrznych (dyskietki, płyty CD, DVD, Internet) nie zawierają wirusów komputerowych,
   4) przestrzegać przepisów o prawie autorskim w części dotyczącej programów komputerowych do pracy tylko na programach oficjalnie zakupionych przez Urząd Miejski - nie instalowania programów pochodzących z innych źródeł, nie udostępniania programów będących własnością Urzędu osobom trzecim,
   5) prawidłowo obsługiwać powierzony sprzęt komputerowy, chronić go przed fizycznym uszkodzeniem (zalanie, zrzucenie itp.) oraz utrzymywać sprzęt w czystości,
   6) nie zmieniać konfiguracji w powierzonym sprzęcie,
   7) niezwłocznie powiadomić informatyka lub ABI o każdym stwierdzonym przypadku naruszenia ochrony zasobów informatycznych, w szczególności danych osobowych, bądź podejrzeniu zainfekowania systemu komputerowego wirusem lub wystąpieniu programów szkodliwych,
   8) informowaniu informatyka lub ABI o wszelkich zaistniałych przypadkach usterek lub niewłaściwym funkcjonowaniu elementów systemu informatycznego,
   9) w razie zaniku napięcia niezwłocznie zamknąć wszystkie programy oraz wyłączyć urządzenia komputerowe do chwili ponownego załączenia zasilania,
   10) prawidłowe rozpoczynanie i kończenie pracy komputera,
   11) właściwa ochrona zasobów systemu informatycznego oraz zewnętrznych nośników informacji.

3. Użytkownikom systemu informatycznego zabrania się:
   1) przetwarzania danych osobowych poza obszarem Urzędu Miejskiego,
   2) samodzielnego dokonywania jakichkolwiek napraw elementów systemu informatycznego,
   3) dokonywania bez wiedzy Informatyka lub ABI jakichkolwiek zmian w rozmieszczeniu sprzętu,

4) korzystania z elementów systemu informatycznego niezgodnie z ich przeznaczeniem,
5) dokonywania jakichkolwiek zmian w konfiguracji systemu operacyjnego, a w szczególności w konfiguracji kont użytkowników, ustawień sieciowych, udostępniania zasobów oraz systemu zabezpieczeń,
6) instalowania, bądź uruchamiania programów, które nie zostały uwzględnione w wykazie oprogramowania zainstalowanego na danym komputerze,
7) podejmowania działań mających na celu uzyskanie nieupoważnionego dostępu do zasobów sieci, a w szczególności przez podszywanie się pod innych użytkowników lub monitorowanie łączy,
8) nieuprawnionego korzystania z zasobów, do których dostęp jest związany z koniecznością posiadania odpowiedniego uprawnienia,
9) umożliwiania osobom nieupoważnionym korzystania z zasobów systemu informatycznego,
10) samowolnego przyłączania, odłączania lub przełączania urządzeń sieciowych,
11) kopiowania oprogramowania i danych na jakiekolwiek nośniki (dyskietki, płyty CD/DVD, pendrive itp.), przenoszenia tego oprogramowania na inne komputery lub przekazywania osobom trzecim bez zgody Burmistrza lub Sekretarza.
12) Zapisu tego nie stosuje się do kopiowania oprogramowania i danych w celu wykonania kopii zapasowych i archiwalnych, zapewnienia ciągłości pracy, eksploatacji oprogramowania zgodnego z warunkami licencji.

§2

Burmistrzowi lub osobie przez niego upoważnionej, przysługuje prawo przeprowadzenia w każdym czasie kontroli sprzętu komputerowego użytkowanego przez pracownika zatrudnionego w Urzędzie Miejskim, a pracownik zobowiązany jest udostępnić ten sprzęt.

§3

Osoby mające dostęp do danych osobowych są zobowiązane do zachowania ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Załącznik Nr 4
do Zarządzenia Nr 78/2012
Burmistrza Sulejowa
z dnia 10 lipca 2012 r.

INSTRUKCJA
W SPRAWIE ZASAD POSTĘPOWANIA W SYTUACJI NARUSZENIA
OCHRONY DANYCH OSOBOWYCH
W URZĘDZIE MIEJSKIM W SULEJOWIE

§1

1. Instrukcja określa tryb postępowania w przypadku gdy:
   1) stwierdzono naruszenie zabezpieczenia danych w systemie informatycznym,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci, mogą wskazywać na naruszenie zabezpieczeń tych danych.

§2

Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, lub podejrzewa naruszenie zabezpieczenia systemu informatycznego w sytuacji, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci, mogą wskazywać na naruszenie zabezpieczenia tych danych, zobowiązana jest niezwłocznie powiadomić o tym Informatyka/Administratora bezpieczeństwa informacji.

§3

Administrator bezpieczeństwa informacji w pierwszej kolejności:
   1) zapisuje wszelkie informacje związane z danym zdarzeniem,
   2) na bieżąco generuje i drukuje (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustalaniu okoliczności zdarzenia,
   3) przystępuje do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metod dostępu do danych osoby niepowołanej.

§4

1. Informatyk/Administrator bezpieczeństwa informacji niezwłocznie podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, poprzez:
   1) fizyczne odłączenie urządzenia,
   2) określenie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
   3) zmianę hasła użytkownika w celu uniknięcia ponownej próby włamania.

§5

Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie.

§6

1. Administrator bezpieczeństwa informacji sprawdza:
    1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
    2) zawartość zbioru danych osobowych,
    3) sposób działania programu,
    4) jakość komunikacji w sieci teleinformatycznej,
    5) obecność wirusów komputerowych.

§7

1. Po dokonaniu powyższych czynności administrator bezpieczeństwa informacji przeprowadza szczegółową analizę stanu systemu informatycznego obejmującą identyfikację:
    1) rodzaju zaistniałego zdarzenia,
    2) metod dostępu do danych osoby nieupoważnionej,
    3) skali zniszczeń.

§8

Informatyk/Administrator bezpieczeństwa informacji przywraca normalny stan działania systemu po czym, jeżeli nastąpiło uszkodzenie bazy danych, odtwarza z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną.

§9

1. Po przywróceniu prawidłowego stanu bazy danych osobowych Informatyk/Administrator bezpieczeństwa informacji przeprowadza szczegółową analizę, w celu określenia przyczyny naruszenia ochrony danych osobowych oraz wykonuje czynności mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
    1) Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, przeprowadzone jest dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych.
    2) Jeżeli przyczyną zdarzenia było uaktywnienie wirusa, ustalane jest źródło pochodzenia oraz wykonywane zabezpieczenie antywirusowe.
    3) Jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, wyciągnięte konsekwencje regulowane ustawą.
    4) Jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, dokonywana jest szczegółowa analiza wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych.
    5) Jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, niezwłocznie przeprowadzana jest kontrola czynności serwisowo – programowych.

§10

Każdorazowo po zaistnieniu przypadków określonych w §1 Informatyk/Administrator bezpieczeństwa informacji przeprowadza analizę ryzyka uwzględniając okoliczności, które spowodowały naruszenie zabezpieczenia.

§11

Administrator bezpieczeństwa informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i przedstawia go Administratorowi danych osobowych.

Załącznik Nr 5
do Zarządzenia Nr 78/2012
Burmistrza Sulejowa
z dnia 10 lipca 2012 r.

Instrukcja postępowania w sprawie zabezpieczenia zbiorów danych w Urzędzie Miejskim w Sulejowie przed pożarem, zalaniem i innym niebezpieczeństwem grożącym zniszczeniem lub utratą zbiorów

§1. Zabezpieczenie zbiorów w Urzędzie Miejskim przed pożarem, zalaniem i innym niebezpieczeństwem polega na:

1) Niedopuszczeniu do sytuacji, w której zbiory mogą zostać utracone, uszkodzone lub zniszczone,
2) ochronie miejsca przechowywania zbiorów.

§2.1. Za właściwe zabezpieczenie zbiorów w Urzędzie Miejskim odpowiada Kierownik ……..

2. Nadzór nad zabezpieczeniem zbiorów w Urzędzie Miejskim sprawuje ……..

§3.1. Każdy pracownik posiadający dostęp do danych osobowych w Urzędzie Miejskim. obowiązany jest:

a) bezzwłocznie powiadomić bezpośredniego przełożonego o wszelkim zagrożeniu dla pozostających w jego dyspozycji zbiorach danych Urzędu,
b) podjąć wszelkie niezbędne środki mające na celu zabezpieczenie posiadanych zbiorów danych (zawiadomić Państwową Straż Pożarną, Policję – w zależności od zaistniałego zagrożenia).

2. Kierownicy komórek organizacyjnych po uzyskaniu informacji od podległych pracowników o zaistniałym zagrożeniu dla zbiorów danych podejmują niezwłocznie działania mające na celu zabezpieczenie sprzętu komputerowego, w którym przechowywane są dane osobowe. Zabezpieczenie polega na wyniesieniu sprzętu z terenu zagrożenia i zabezpieczenia go przed pożarem, zalaniem i innym niebezpieczeństwem.

3. Równocześnie z podjęciem działań kierownicy komórek organizacyjnych Urzędu Miejskiego o zaistniałej sytuacji zawiadamiają Burmistrza i …….

4. Kierownik ……. sprawuje bezpośrednia kontrolę nad właściwym zabezpieczeniem zbiorów danych w Urzędzie Miejskim oraz koordynuje wszelkimi działaniami w Urzędzie w przypadku zagrożenia tych danych.

5. Kierownik …….. zobowiązany jest przedłożyć Burmistrzowi sprawozdanie z przebiegu podjętych działań zmierzających do prawidłowego zabezpieczenia zbiorów danych.

6. Telefony na wypadek zagrożenia:

1) Burmistrz – ……..
2) ……..
3) ……..