Zarządzenie Nr 109/2009

Burmistrza Miasta i Gminy Baranów Sandomierski
z dnia 31 sierpnia 2009r.

w sprawie zmiany zarządzenia nr 18/2007 w sprawie wprowadzenia Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Baranów Sandomierski.

Na podstawie art. 33 ust. 2 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2001r. Nr 142, poz.1591 z późn. zmian.) w związku z paragrafem 3 ust. 1 Rozporządzenia Rady Ministrów z dnia 11 października 2005r w sprawie minimalnych wymagań dla systemów teleinformatycznych
(Dz. U. z 2005 Nr 212 poz. 1766)

zarządzam, co następuje:

§ 1

Załączniki nr 1 uchwały nr 18/2007 otrzymuje nowe brzmienie zgodnie z załącznikiem nr 1 do niniejszej uchwały.

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia.

§ 3

Wykonanie zarządzenia powierza się Sekretarzowi Gminy Baranów Sandomierski.

BURMISTRZ
Mirosław Pluta

Załącznik nr 1
do Zarządzenia nr 109/2009
z dnia 31 sierpnia 2009r.

Polityka bezpieczeństwa

i instrukcja zarządzania systemem informatycznym

służącym do przetwarzania danych osobowych

w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Opracował:
Tomasz Pruś – Informatyk

Sierpień 2009 r.

Spis treści

WPROWADZENIE

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:
1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r.Nr 101, poz. 926 z późniejszymi zmianami),
2) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. Nr 11, poz. 95 z późn. zm.),
3) ustawą z dnia 29 września 1994r. o rachunkowości (tekst jednolity Dz. U. z 2002r Nr. 76 poz 694 z późniejszymi zmianami),
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. Nr 100, poz. 1024),

Niniejszy dokument reguluje sprawy ochrony danych osobowych zawartych w systemie informatycznym eksploatowanym w lokalnej sieci komputerowej Microsoft Windows Network (MWN) oraz zbiorów danych zapisanych w postaci dokumentacji papierowej w Urzędzie Miasta i Gminy w Baranowie Sandomierskim w dalszej części opracowania zwanym jako Urząd .
Instrukcja dotyczy następujących niżej wymienionych baz danych:
Ewidencja ludności,
Urząd Stanu Cywilnego,
Podatki,
Świadczenia rodzinne,
Stypendia Szkolne
Planowanie budżetu
Księgowość
Płace

Do przetwarzania zbiorów danych zawierających dane osobowe stosuje się następujące programy:
zbiór „Ewidencja ludności i dowodów osobistych" – przy użyciu programu „ELUD+" i „WYB+" firmy Radix z bazą danych na SBS 2003 PL
zbiór „Urząd Stanu Cywilnego" – przy użyciu programu „PB_USC" firmy Technika
zbiór „Podatki" – przy użyciu programu „EGRUN" , „POGRUN+" i „WIP+" firmy Radix z bazą danych na SBS 2003 PL (.dbf oraz SQL)
zbiór „Świadczenia Rodzinne" – przy użyciu programu „EZAR+", „FA+" i „WIP" firmy Radix z bazą danych na SBS 2003 PL
zbiór „Stypendia Szkolne" – przy użyciu programu "ESO+" firmy Radix z bazą danych na SBS 2003 PL
zbór „Księgowość" – przy użyciu programu „FKB+" firmy Radix z bazą danych na SBS 2003 PL
zbiór „Płace" – przy użyciu programu „PŁACE+" firmy Radix oraz program Płatnik z bazą danych na SBS 2003 PL
zbiór „Kadry" – przy użyciu programu „KADRY+" firmy Radix oraz program Płatnik z bazą danych na SBS 2003 PL

Osobami przetwarzającymi dane osobowe w zakresie:
programu „ELUD+", „WYB+" jest referent ds. ewidencji ludności,
programu „PB_ USC" jest Kierownik Urzędu Stanu Cywilnego,
programu „EGRUN", „POGRUN+" i „WIP+" są inspektorzy: ds. księgowości podatkowej oraz wymiaru podatków i opłat lokalnych,
programu „EZAR+", „FA+" i „WIP+" – jest pracownik ds. realizacji świadczeń rodzinnych
programu „ESO+" jest pracownik ds. realizacji stypendiów szkolnych
programu „Bestia" jest Kierownik referatu Finansów
programu „FKB" są pracownicy ds. księgowości
programu „Płace" są pracownicy ds. księgowości
programu „Kadry" są pracownicy ds. kadr

Opis struktur zbiorów danych jest zawarty w Załączniku Nr 5 do niniejszego dokumentu. Granice obszarów, w których przetwarzane są dane osobowe zostały opisane w Załączniku Nr 6.
Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.
Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób zabezpieczenia systemów informatycznych postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.
Potrzeba jego opracowania wynika z § 3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18 póz. 162) oraz § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, póz. 1024).
1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
stwierdzono naruszenie zabezpieczenia systemu informatycznego,
stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Miasta i Gminy w Baranowie Sandomierskim
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym Urzędu.
4. Administrator Danych, którym jest Burmistrz Miasta i Gminy Baranów Sandomierski zwanym dalej Burmistrzem, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej

„Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa".
5. „Administrator Bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:
ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.
7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

1. OPIS PROGRAMÓW KOMPUTEROWYCH

1.1 ELUD+

System Ewidencji Ludności ELUD+ jest wersją systemu ELUD przeznaczoną do pracy w środowisku Microsoft Windows NT/200x/XP/Vista, z wykorzystaniem serwera baz danych. System ELUD+ posiada homologację Departamentu Rozwoju Informatyki i Systemu Rejestrów Państwowych MSWiA ważną do dnia 31 lipca 2011 r.

Przeznaczenie
System ELUD+ posiada homologację Departamentu Rozwoju Informatyki i Systemu Rejestrów Państwowych MSWiA. Przeznaczony jest do obsługi Lokalnego Banku Danych PESEL w zakresie zadań wykonywanych przez gminę, w tym:

•rejestracja i modyfikacja danych dotyczących ludności w układzie kart osobowych mieszkańców,
•emisja wymaganych przepisami dokumentów i wykazów,
•przeprowadzanie analiz i sprawozdawczości oraz emisja wyników,
•utrzymywanie i konserwacja bazy aktualnych i byłych mieszkańców,
•prowadzenie kartotek obwodów wyborczych oraz sporządzenie list wyborczych,
•okresowa wymiana danych z systemami nadrzędnymi: Rejestrem PESEL-CBD, Wojewódzkim Bankiem Danych, Terenowym Bankiem Danych,
•udostępnianie danych dotyczących ludności pozostałym systemom z pakietu RADIX oraz współpraca z innymi systemami pakietu RADIX.

Współpraca z innymi systemami pakietu RADIX:
•System Wydawania Zezwoleń ALK+
•System Ewidencji Działalności Gospodarczej EPOD+
•System Obsługi Stypendiów Oświatowych ESO+
•System Obsługi Świadczeń Rodzinnych EZAR+
•System Obsługi Funduszu Alimentacyjnego FA+
•System Fakturowania VAT FAKTURA+
•System Obsługi Kadr KADRY+
•System Obsługi Kasy KASA+
•System Naliczania Dodatków Mieszkaniowych NDM+
•System Płacowy PŁACE+
•System Naliczania Podatków od Gruntów i Nieruchomości POGRUN+
•System Naliczania Podatków od Środków Transportu POST
•System Obsługi Rejestrów i Umów REJ+
•System Stanu Cywilnego USC+
•System Windykacji Opłat i Podatków WIP+
•Rejestr Wyborców WYB+
Platforma systemowa
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL,
•system jest też dostępny w wersji dla MS-DOS/Windows/dbf.

1.2 WYB+

System Rejestr Wyborców WYB+ jest wersją systemu WYB przeznaczoną do pracy w środowisku Microsoft Windows NT/200x/XP/Vista/7, z wykorzystaniem serwera baz danych.

Przeznaczenie
System WYB+ przeznaczony jest do:

•prowadzenia stałego rejestru wyborców,

•emitowania spisu wyborców,
•drukowania zawiadomień związanych z prowadzeniem rejestru wyborców,
•sporządzania meldunków dla PKW.
Rejestr wyborców jest prowadzony w oparciu o dane zawarte w bazie ewidencji ludności systemu ELUD+ oraz o dane zarejestrowane na wniosek wyborcy. Na podstawie danych zawartych w Systemie Ewidencji Ludności ELUD+ przeprowadzana jest automatyczna selekcja osób zameldowanych na pobyt stały, które ukończyły 18 lat i przeniesienie ich do bazy osób wpisanych z urzędu.

System WYB+ współpracuje z innymi systemami pakietu RADIX.

Współpraca z innymi systemami pakietu RADIX
•System Ewidencji Ludności ELUD
•System Ewidencji Ludności ELUD+
•System Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO
Platforma systemowa
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL,
•system jest też dostępny w wersji dla MS-DOS/Windows/dbf.

1.3 PB_USC

Wymagania aplikacji PB_USC

•Akceptowany system operacyjny dla aplikacji to Windows Vista, WindowsXP, Windows2003 i wyższe. Zaleca się Windows Vista.
Aplikacja nie działa na Windows98 i Windows2000.
W związku z postępującym rozwojem systemów operacyjnych i narzędzia do budowy aplikacji firma Sybase zaprzestała dostosowywania Power Buildera do starszych systemów operacyjnych Microsoft. Stąd najnowsze wersje aplikacji napisane w Power Builder nie zadziałają na przykład na Win98 i Win2000. Nasza firma utrzymywała kompatybilność aplikacji dla USC z tymi systemami do końca czerwca 2005 roku.

•Zalecana minimalna rozdzielczość ekranu 1024x768. Zaleca się 1280x1024 monitor LCD 19". Program zadziała na rozdzielczości od 800x600, jednak odradzamy pracę w takich rozdzielczościach.

•Zalecany rozmiar pamięci operacyjnej to 2048MB, minimum 1024MB.
Zalecana szybkość procesora to minimum Celeron 2GHz. Program zadziała na komputerze z dowolnym procesorem, jednak jego szybkość może dla pewnych funkcji budzić irytację.
Wymagane wolne miejsce na dysku przed instalacją to co najmniej 50MB.

•Zalecane wolne miejsce na dysku w czasie pracy to minimum 50MB.

•Baza danych typu SQL mająca sterowniki ODBC. Nie zalecamy pracy z bazą Access pomimo tego, że program z nią w pełni współpracuje. Nie zalecamy baz FireBird, InterBase.

•Baza danych nie powinna reagować na wielkość znaków w nazwach pól tabel.

•Ponieważ aplikacja łączy się z bazą danych otwierając dwie tranzakcje na sesję fakt ten należy uwzględnić przy licencjonowaniu bazy danych ze względu na liczbę dopuszczalnych połączeń.

•Zalecany porządek sortowania w bazie to strona kodowa Windows (WIN1250). Można użyć dowolnego trybu sortowania znaków narodowych.

•Zaleca się, by baza danych raz na miesiąc była kopiowana na nośnik trwały.

•Ze względu na fakt, że akty w usc. leżą 100 lat zaleca się, by drukarki używane przez system były igłowe. Drukarki igłowe obecnie mają najwyższą trwałość wydruku. Zaleca się, by ilość igieł wynosiła 24. PROSZĘ PAMIĘTAĆ O TYM, ŻE DRUKOWANE AKTY MAJĄ ROZMIAR WIĘKSZY NIŻ A4. PROSZĘ ZAKUPIĆ DRUKARKI Z 15" WAŁKIEM NA STANOWISKA PROWADZĄCE REJESTRACJĘ.

•Użycie konfiguracji sprzętowej o wymaganiach niższych niż podane może znacznie zwolnić lub nawet uniemożliwić uruchomienie aplikacji.

Bazy danych z którymi program współpracuje
•Aplikacja obecnie pracuje i przeszła wszystkie testy na następujących bazach danych:
Oracle
Microsoft SQL Server
Adaptive Server Anywhere
MySQL.
Microsoft Access (mimo to nie zalecamy pracy na tej bazie)

•Aplikacja nie była testowana z następującymi bazami danych:
Firebird, InterBase. Jeśli to możliwe zalecamy nie decydować się na te bazy.

1.4 POGRUN +

System Naliczania Podatków od Gruntów i Nieruchomości POGRUN+ jest wersją systemu POGRUN przeznaczoną do pracy w środowisku Microsoft Windows NT/2000/XP/Vista/7, z wykorzystaniem serwera baz danych.

Przeznaczenie
System POGRUN+ przeznaczony jest do:

•prowadzenia pełnej ewidencji gospodarstw rolnych, lasów oraz nieruchomości, zarówno będących własnością osób fizycznych, jak prawnych i innych (deklaracje podatkowe),
•ustalenia wymiaru podatku rolnego, leśnego i od nieruchomości,
•wprowadzania zmian i ustalenia związanych z nimi przypisów i odpisów,
•wydruku postanowień o wszczęciu postępowania podatkowego, nakazów płatniczych, decyzji po zmianie i decyzji wymiarowych,
•prowadzenia pełnej obsługi i wydawania zaświadczeń na bony paliwowe,
•drukowania rejestrów, zaświadczeń, wykazów oraz sprawozdań okresowych i rocznych,

•prowadzenia wieloletniego archiwum wymiaru.
System współpracuje z innymi systemami pakietu RADIX.

Współpraca z innymi systemami pakietu RADIX
•System Ewidencji Gruntów i Mienia Komunalnego EGRUN
•System Ewidencji Ludności ELUD
•System Ewidencji Ludności ELUD+
•System Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO
•System Obsługi Rejestrów i Umów REJ+
•System Windykacji Opłat i Podatków WIP+
Platforma systemowa.
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL,
•system jest też dostępny w wersji dla MS-DOS/Windows/dbf.

1.5 EGRUN

System Ewidencji Mienia Komunalnego EGRUN służy do prowadzenia ewidencji gruntów i budynków w układzie rejestru gruntów i budynków dostosowanym do aktualnie obowiązujących przepisów, prowadzenia pełnej ewidencji mienia komunalnego, archiwizacji jednostek rejestrowych oraz sporządzania zestawień ewidencji gruntów i typowych raportów dotyczących mienia komunalnego. Dodatkowo system umożliwia tworzenie i wczytywanie plików bazy danych w formacie SWDE przeznaczonych do komunikacji z innymi systemami ewidencji gruntów.

Przeznaczenie
System Ewidencji Mienia Komunalnego EGRUN przeznaczony jest do kompleksowej obsługi ewidencji gruntów i budynków, w tym ewidencji mienia komunalnego: gruntów, budynków i innych obiektów (np. drogi, wodociągi).

System EGRUN umożliwia:

•prowadzenie pełnej ewidencji gruntów i budynków, w układzie rejestru gruntów i budynków dostosowanym do aktualnie obowiązujących przepisów,
•prowadzenie pełnej ewidencji mienia komunalnego,
•sporządzanie wymaganych przepisami raportów oraz zestawień i wykazów ewidencji gruntów, budynków i mienia komunalnego,
•prowadzenie wieloletniego archiwum jednostek rejestrowych.
Dodatkowe możliwości:

•tworzenie i wczytywanie plików w formacie SWDE umożliwiających przejmowanie baz danych z innych systemów ewidencji gruntów oraz przekazywanie danych zarejestrowanych w systemie EGRUN.
System współpracuje z innymi systemami pakietu RADIX.

Współpraca z innymi systemami pakietu RADIX
•System Ewidencji Budynków i Naliczania Czynszów EBUD
•System Naliczania Opłat Za Użytkowanie Wieczyste Gruntów EGW
•System Ewidencji Ludności ELUD
•System Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO

•System Naliczania Podatków od Gruntów i Nieruchomości POGRUN
•System Naliczania Podatków od Gruntów i Nieruchomości POGRUN+
•System Nadawania Uprawnień UPR
•System Windykacji Opłat i Podatków WIP+
Platforma systemowa
•Microsoft DOS/Windows, Novell NetWare.

1.6 EZAR+

System Obsługi Świadczeń Rodzinnych EZAR+ powstał w celu ułatwienia pracy Urzędom i Instytucjom zajmującym się obsługą świadczeń rodzinnych zgodnie z postanowieniami Ustawy z dnia 28 listopada 2003 roku o świadczeniach rodzinnych (Dz.U. 2003 nr 228, poz. 2255).

Przeznaczenie
System EZAR+ umożliwia:

Rejestrowanie i prowadzenie ewidencji
•rejestrowanie i prowadzenie ewidencji wszystkich typów wniosków o świadczenia rodzinne;
•rejestrowanie i prowadzenia ewidencji związanych ze składanymi wnioskami załączników;
•rejestrowanie i prowadzenie ewidencji wnioskodawców, osób pobierających świadczenia oraz członków rodzin wraz z zaświadczeniami o dochodach;
Wystawianie decyzji
•rodzaj i liczba świadczeń podpowiadane są automatycznie przez system, w zależności od typu składanego wniosku i danych świadczeniobiorców (np. wiek, stopień niepełnosprawności);
•treść decyzji podpowiadana jest automatycznie przez system po kontroli złożenia wszystkich wymaganych załączników, w zależności od naliczonej kwoty dochodów na członka rodziny oraz danych świadczeniobiorców (np. wiek, stopień niepełnosprawności).
W systemie istnieje możliwość sparametryzowania wymagalności dokumentów poszczególnych rodzajów w zależności od składanego wniosku.

Wypłaty zasiłków
EZAR+ umożliwia sporządzenie i wydrukowanie:

•list wypłat,
•przekazów pieniężnych pocztowych;
•druków przelewów na konta świadczeniobiorców.
Od wypłacanych zasiłków automatycznie naliczane są właściwe składki ZUS, a następnie odpowiednie dokumenty ZUS są sporządzane i przekazywane do Programu Płatnika.

Sprawozdawczość
Sporządzanie i wydruk: Sprawozdania rzeczowo-finansowego o zrealizowanych zadaniach z ustawy o świadczeniach rodzinnych.

Współpraca z innymi systemami

•Przejmowanie danych osobowych wnioskodawców i członków ich rodzin z Systemu Ewidencji Ludności ELUD (wersja DOS) oraz ELUD+ (wersja SQL) i z Systemu Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO+.

•przekazywanie dokumentów ZUS (np. RCA) do Programu Płatnika
Współpraca z innymi systemami pakietu RADIX
•System Ewidencji Ludności ELUD
•System Ewidencji Ludności ELUD+
•System Obsługi Stypendiów Oświatowych ESO+
•System Obsługi Funduszu Alimentacyjnego FA+
•System Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO
•System Windykacji Opłat i Podatków WIP+
Platforma systemowa
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL.

1.7 ESO+

System Obsługi Stypendiów Oświatowych ESO+ przeznaczony jest do obsługi zadań związanych z przyznawaniem i realizacją stypendiów oświatowych - socjalnych oraz motywacyjnych, a także zasiłków jednorazowych, zgodnie z Ustawą z dnia 16 grudnia 2004 r. o zmianie ustawy o systemie oświaty oraz ustawy o podatku dochodowym od osób fizycznych (Dziennik Ustaw Nr 281, Pozycja 2781) i rozporządzeniami do tej ustawy.

Podstawowe operacje systemu
Rejestrowanie i prowadzenie ewidencji:
•wszystkich wniosków o stypendia oraz zasiłki jednorazowe;
•związanych ze składanymi wnioskami załączników;
•wnioskodawców oraz członków ich rodzin wraz z zaświadczeniami o dochodach;
•dysponentów świadczeń;
•wnioskowanych i przyznanych świadczeń wraz z rejestracją i ewidencją dokumentów rozliczających (faktury, rachunki itp.).

Wystawianie decyzji
•treść decyzji podpowiadana jest automatycznie przez system, w zależności od naliczonej kwoty dochodów na członka rodziny, danych świadczeniobiorców, rodzaju przyznanych świadczeń oraz dysponentów.
Wypłaty stypendiów i zasiłków
ESO+ umożliwia sporządzenie i wydrukowanie:

•list wypłat,
•przekazów pieniężnych pocztowych;
•druków przelewów na konta świadczeniobiorców.

Współpraca z innymi systemami

•Przejmowanie danych osobowych wnioskodawców i ich rodzin z Systemu Ewidencji Ludności ELUD (wersja DOS) oraz ELUD+ (wersja SQL) i z Systemu Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO+.
•Przejmowanie danych osobowych wnioskodawców i ich rodzin z Systemu Obsługi Świadczeń Rodzinnych EZAR+.
Współpraca z innymi systemami pakietu RADIX
•System Ewidencji Ludności ELUD
•System Ewidencji Ludności ELUD+
•System Obsługi Świadczeń Rodzinnych EZAR+

•System Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO
Platforma systemowa
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL.

1.8 FA+

System Obsługi Funduszu Alimentacyjnego FA+ służy do obsługi funkcji związanych z przyznawaniem i realizacją świadczeń z funduszu alimentacyjnego, zgodnie z ustawą o pomocy osobom uprawnionym do alimentów (Dz. U. z 2007 r. Nr 192, poz. 1378).

Przeznaczenie
Ewidencja
•wniosków o świadczenia z funduszu alimentacyjnego,
•wniosków o podejmowanie działań wobec dłużników alimentacyjnych,
•wnioskodawców, osób uprawnionych oraz członków rodzin wraz z zaświadczeniami o dochodach,
•związanej z wnioskami korespondencji wraz z załącznikami,
•wydanych decyzji,
•wywiadów alimentacyjnych i oświadczeń majątkowych dłużników,
•wypłaconych świadczeń.
Obsługa wypłat
FA+ umożliwia sporządzenie i drukowanie:

•list wypłat,
•przekazów pieniężnych,
•druków przelewów na konta świadczeniobiorców.
Sprawozdawczość
FA+ umożliwia sporządzenie i drukowanie sprawozdań rzeczowo-finansowych o realizacji ustawy o pomocy osobom uprawnionym do alimentów.

Współpraca z innymi systemami pakietu RADIX
•System Ewidencji Ludności ELUD
•System Ewidencji Ludności ELUD+
•System Obsługi Świadczeń Rodzinnych EZAR+
•System Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO
•System Windykacji Opłat i Podatków WIP+
Platforma systemowa
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL.

1.9 FKB+

System Księgowości Budżetowej FKB+ jest wersją systemu FKB przeznaczoną do pracy w środowisku Microsoft Windows NT/200x/XP/Vista/7, z wykorzystaniem serwera baz danych.

Przeznaczenie
System FKB+ przeznaczony jest do:

•rejestracji, księgowania i drukowania dowodów księgowych, w tym operacji związanych z podatkiem VAT,

•zakładania, rozszerzania i modyfikowania planu kont,
•prowadzenia kartoteki obrotów wg obowiązującej klasyfikacji budżetowej,
•sporządzania i drukowania wymaganych wykazów i sprawozdań na dany dzień, w ujęciu analitycznym lub syntetycznym, wg dowolnego układu klasyfikacji budżetowej, w tym sprawozdań kwartalnych i rocznych;
•przeglądania i drukowania dziennika obrotów, wykazów obrotów i stanów kont za dowolny okres czasu, w ujęciu analitycznym i syntetycznym,
•zakładania i przeglądania archiwum lat ubiegłych wg zasad określonych ustawą o rachunkowości.
System szeroko współpracuje z innymi pakietami z systemu RADIX, także w ramach operacji księgowych.

Współpraca z innymi systemami pakietu RADIX
•System Fakturowania VAT FAKTURA
•System Fakturowania VAT FAKTURA+
•System Obsługi Kasy KASA
•System Obsługi Kasy KASA+
•System Naliczania Płac PŁACE
•System Płacowy PŁACE+
•System Windykacji Opłat i Podatków WIP
•System Windykacji Opłat i Podatków WIP+
Platforma systemowa
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL,
•system jest też dostępny w wersji dla MS-DOS/Windows/dbf.

1.10 PŁACE+

System PŁACE+, we współpracy z systemem KADRY+, służy do automatycznego sporządzania list płac zatrudnionych pracowników i drukowania zestawień płacowych.

Przeznaczenie
System PŁACE przeznaczony jest do:

•automatycznego sporządzania oraz drukowania list płac zatrudnionych pracowników
•obsługi składek ubezpieczeniowych wg zasad zgodnych z reformą ubezpieczeń społecznych
•automatycznego prowadzenia kartotek kasy zapomogowo-pożyczkowej i funduszu mieszkaniowego
•drukowania zestawień płacowych, odcinków wypłat, odcinków ZUS oraz dowolnych zaświadczeń i wykazów, także wg klasyfikacji budżetowej
•automatycznego naliczania zasiłków
•prowadzenia kart zasiłkowych i deklaracji rozliczeniowych ZUS
•emitowania odpowiednich dokumentów do programu Płatnik ZUS
•prowadzenia wieloletniego archiwum.
W wersji wielozadaniowej systemu, przy współpracy z wersją wielozadaniową systemu KADRY+, możliwe jest zarejestrowanie i osobna obsługa wielu zadań budżetowych (niezależnych jednostek budżetowych).

System współpracuje z innymi systemami pakietu RADIX.

Współpraca z innymi systemami pakietu RADIX

•System Ewidencji Ludności ELUD+
•System Finansowo-Księgowy Księgowości Budżetowej FKB+
•System Obsługi Kadr KADRY+
Platforma systemowa
•Stacja robocza: system operacyjny Linux lub Windows (zalecana przeglądarka Firefox, dopuszczalna Internet Explorer lub Opera),
•serwer: serwer bazy danych PostgreSQL lub Microsoft SQL Server oraz serwer aplikacji Apache Tomcat,
•system jest też dostępny w wersji dla MS-DOS/Windows/dbf.

1.11 KADRY+

System KADRY+ służy do rejestracji danych osobowych pracowników, prowadzenia kartotek zawierających warunki i zasady zatrudnienia, przebieg pracy zawodowej, dane do ubezpieczenia ZUS i inne, prowadzenia ewidencji czasu pracy, drukowania dokumentów związanych z zatrudnieniem, automatycznego aktualizowania danych związanych z liczbą lat stażu pracy, należnym dodatkiem stażowym, nagrodą jubileuszową, wykonywania dowolnych analiz i wyciągów z bazy danych na podstawie określonych przez użytkownika warunków wyboru, a w powiązaniu z systemem PŁACE+, również do automatycznego sporządzania list płac, wykazów podatkowych itp.

Przeznaczenie
System KADRY przeznaczony jest do:

•rejestracji danych pracowników oraz prowadzenia kartotek zawierających ich dane osobowe, warunki i zasady zatrudnienia, przebieg pracy zatrudnionych pracowników, dane do ubezpieczenia ZUS i inne,
•prowadzenia ewidencji czasu pracy,
•drukowania dokumentów związanych z zatrudnieniem,
•automatycznego aktualizowania danych związanych z liczbą lat stażu pracy, należnym dodatkiem stażowym, nagrodą jubileuszową,
•archiwizowania danych pracowników, w tym pracowników zwolnionych,
•wykonywania analiz i wyciągów z bazy danych na podstawie określonych przez użytkownika warunków wyboru danych,
•w powiązaniu z systemem PŁACE+ - automatycznego sporządzania list płac, wykazów podatkowych itp,
•prowadzenia wieloletniego archiwum.
W wersji wielozadaniowej systemu możliwe jest zarejestrowanie i osobna obsługa do 99 zadań budżetowych (niezależnych jednostek budżetowych).

System współpracuje z innymi systemami pakietu RADIX.

Współpraca z innymi systemami pakietu RADIX
•System Ewidencji Ludności ELUD+
•System Płacowy PŁACE+
Platforma systemowa
•Stacja robocza: system operacyjny Linux lub Windows (zalecana przeglądarka Firefox, dopuszczalna Internet Explorer lub Opera),
•serwer: serwer bazy danych PostgreSQL lub Microsoft SQL Server oraz serwer aplikacji Apache Tomcat,
•system jest też dostępny w wersji dla MS-DOS/Windows/dbf.

1.12 WIP+

System Windykacji Opłat i Podatków WIP+ jest wersją systemu WIP przeznaczoną do pracy w środowisku Microsoft Windows NT/200x/XP/Vista/7, z wykorzystaniem serwera baz danych.

Przeznaczenie
System WIP+ przeznaczony jest do:

•zakładania i bieżącej aktualizacji kont dla wszystkich podatników z terenu miasta/gminy,
•analizy rozrachunkowej kont,
•obsługi tytułów wykonawczych,
•drukowania upomnień, decyzji itp.
•tworzenia i drukowania wykazów podatników oraz podatków,
•prowadzenia wieloletniego archiwum wraz z możliwością jego przeglądania.
System współpracuje z innymi systemami pakietu RADIX, przejmując dane osobowe oraz naliczone w systemach wymiarowych przypisy i należności.

Współpraca z innymi systemami pakietu RADIX
•System Wydawania Zezwoleń ALK
•System Wydawania Zezwoleń ALK+
•System Ewidencji Budynków i Naliczania Czynszów EBUD
•System Ewidencji Gruntów i Mienia Komunalnego EGRUN
•System Naliczania Opłat Za Użytkowanie Wieczyste Gruntów EGW
•System Ewidencji Opłat Komunalnych EKO
•System Ewidencji Ludności ELUD
•System Ewidencji Ludności ELUD+
•System Obsługi Świadczeń Rodzinnych EZAR+
•System Obsługi Funduszu Alimentacyjnego FA+
•System Fakturowania VAT FAKTURA
•System Fakturowania VAT FAKTURA+
•System Finansowo-Księgowy Księgowości Budżetowej FKB+
•System Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO
•System Obsługi Kasy KASA+
•System Naliczania Podatków od Gruntów i Nieruchomości POGRUN+
•System Naliczania Podatków od Środków Transportu POST
•System Obsługi Rejestrów i Umów REJ+
•System Straż Miejska STM
Platforma systemowa
•System operacyjny Microsoft Windows 200x/XP/Vista/7,
•serwer bazy danych Oracle, Microsoft SQL Server lub PostgreSQL,
•system jest też dostępny w wersji dla MS-DOS/Windows/dbf.

2. DATA INSTALACJI PROGRAMÓW

Programy komputerowe w wersji SQL były zakupione następnie udostępnione pracownikom aby mogli zapoznać się z funkcjami programu, po tym okresie zazwyczaj na przełomie roku był uruchamiany właściwy program w wersji „+"(z bazą danych SQL) .

L.p.	Nazwa programu	wersja	Data instalacji
1.	EGRUN	8.06	2005-12-12
2.	ELUD	3.03	1996-03-04
3.	ELUD+	2.04	2007-10-25
4.	ESO+	1.02	2005-06-15
5.	EZAR+	1.01	2004-05-19
6.	FA+	1.01	2008-08-14
7.	FKB	3.12	1996-07-16
8.	FKB+	2.05	2007-12-19
9.	KADRY	3.06	1995-11-16
10.	KADRY+	1.01	2007-12-19
11.	PŁACE	5.01	1995-11-16
12.	PŁACE+	1.01	2007-12-19
13.	POGRUN	4.09	1996-11-22
14.	POGRUN+	2.06	2007-10-25
15.	POST	1.01	2002-02-09
16.	WIP	4.02	1997-03-31
17.	WIP+	3.02	2007-10-25
18.	WYB	3.02	2005-09-21
19.	WYB+	3.10	2007-10-25
20.	PB_USC	6.00	2008-01-01

3. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:
zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
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.,
niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie

wykonanie w określonym terminie kopii oraz prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

4. ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 1.

Cele i zasady ogólne

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu jest Burmistrz.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:
zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
zapobiegać zabraniu danych przez osobę nieuprawnioną,
zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych. Szczegółowe obowiązki Administratora Danych zawarte są w Załączniku Nr 1.

§ 2.
Cele ochrony i zasady ogólne

1. Celem wprowadzonych niniejszą Polityką zabezpieczeń i obostrzeń jest ochrona danych osobowych zawartych w eksploatowanym w sieci Microsoft Windows Network systemie. Określone niżej sposoby zabezpieczeń dotyczą:
1.1 zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień,
1.2 ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych.
1.3 systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń pracowników, personelu pomocniczego Urzędu oraz serwisu zewnętrznego,
1.4 monitorowania systemu zabezpieczeń,
1.5 zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych.

2. Strategia ochrony danych osobowych opiera się na następujących zasadach:
2.1 fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy informatyczne blokują drzwi.
2.2 podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym.
2.3 dodatkowym systemem zabezpieczenia jest stosowanie kryptograficznej ochrony danych, jaką oferuje system operacyjny.
2.4 dodatkowe kopie danych zarchiwizowanych na nośnikach magnetycznych lub płytach CD są przechowywane w oddzielnym budynku – chronią w ten sposób dane na wypadek pożaru, klęski żywiołowej lub katastrofy. Prowadzona jest ścisła ewidencja tych nośników,
2.5 w pomieszczeniach, w których zainstalowany jest serwer i komputery zawierające bazy danych jest zainstalowany system alarmowy, pomieszczenie wyposażone jest w gaśnice,

2.6 zagadnienia związane z ochrona danych i obowiązki stąd wynikające są ujęte w zakresach czynności pracowników stanowiące Załącznik Nr 3,
2.7 każdy pracownik Urzędu podpisze oświadczenie stanowiące Załącznik Nr 4,
2.8 za całość polityki bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji.

§ 3.

Zabezpieczenia

Wprowadza się następujące zabezpieczenia danych w systemie informatycznym:
Na wszystkich stacja roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom zabezpieczeń.
Pomieszczenia, w których stoi serwer i komputery zawierające dane osobowe i kartoteki osobowe są zabezpieczone poprzez system alarmowy, pomieszczenie nie posiada okien.
Wykaz tych pomieszczeń zawiera Załącznik Nr 6.
Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
Uruchomienie stacji roboczych, na których przetwarzane są dane osobowe wymaga podania hasła BIOS-u,
Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji. Nieudane próby logowania są rejestrowane, a po 3 nieudanych próbach logowania następuje czasowa blokada konta.
Logowanie do systemu możliwe jest tylko w godzinach pracy Urzędu.
Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
Administrator Bezpieczeństwa Informacji ma uprawnienia do definiowania kont użytkowników i haseł.
Wykorzystany jest system szyfrowania danych (dostępny w systemie operacyjnym) uniemożliwiający odczyt danych osobom nieupoważnionym.
W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej dostępnej w systemie operacyjnym.
Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe. Za aktualizację bazy wirusów odpowiada użytkownik.
Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
Kopie bezpieczeństwa na nośnikach optycznych wykonują okresowo pracownicy w ramach swoich obowiązków. Kopie bezpieczeństwa przechowywane są w kasie pancernej w serwerowni.. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
Kartoteki papierowe znajdują się w meblowych szafach, zamykanych na zamki meblowe w pokojach, w których przetwarzane dane osobowe.
Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:
dostęp do danych mają wyłącznie pracownicy wyznaczeni przez Administratora Danych.
Administrator Danych prowadzi ścisły rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych, łącznie z ich identyfikatorami w systemie.
w pokoju, do którego dostęp mają petenci monitory komputerowe w miarę możliwości ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie,
w przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacie ekranu, których deaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.
częstotliwość tworzenia kopii bezpieczeństwa określa instrukcja archiwowania zasobów. Za wykonanie tych kopii odpowiedzialne są osoby przetwarzające dane osobowe..

tworzeniem kopii bezpieczeństwa na nośnikach optycznych (płyty CD-R/CD-RW) zajmuje się informatyk.

§ 4.

Monitorowanie zabezpieczeń

Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:
Administrator Danych
Administrator Bezpieczeństwa Informacji

W ramach monitoringu należy przeprowadzać następujące działania:
okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
kontrola ewidencji nośników magnetycznych i optycznych,
sprawdzania częstotliwości zmian haseł,
Administrator Bezpieczeństwa może zarządzić kontrole zatwierdzoną przez Administratora Danych i zgodnie z nim przeprowadza kontrole oraz dokonuje ocen stanu bezpieczeństwa danych osobowych.
Na podstawie zgromadzonych materiałów, o których mowa w pkt. 3. Administrator sporządza roczne sprawozdanie i przedstawia Administratorowi Danych.

§ 5.

Szkolenia

Szkolenie podstawowe dotyczące bezpieczeństwa danych obejmuje wszystkich pracowników Urzędu,
System szkoleń szczegółowych obejmuje pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych.
Tematyka szkoleń obejmuje:
przepisy i instrukcje wewnętrzne dotyczące ochrony danych archiwizacji zasobów i przechowywania nośników, niszczenie wydruków i zapisów na nośnikach magnetycznych i optycznych,
zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.

§ 6.

Archiwowanie danych

Dane systemów kopiowane są w trybie tygodniowym. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane.
Dodatkowo na koniec każdego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przekazywane są do szafy pancernej w serwerowi Urzedu.
Dyskietki, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, aby nie można było odtworzyć ich zawartości. Płyty CD, na których przechowuje się kopie awaryjne niszczy się trwale w sposób mechaniczny.

Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza informatyk.

§ 7.

Niszczenie wydruków i zapisów na nośnikach magnetycznych

Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa.
Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać itp.).
Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarce

Rozdział 3

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik Urzędu, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:
niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
udokumentować wstępnie zaistniałe naruszenie,
nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4 Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:
zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,
nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.
5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego Załącznik Nr 7, który powinien zawierać w szczególności:
wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpowiedzialnych w związku z naruszeniem,
określenie czasu i miejsca naruszenia i powiadomienia,
określenie okoliczności towarzyszących i rodzaju naruszenia,
wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,

wstępną ocenę przyczyn wystąpienia naruszenia,
ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych (Burmistrzowi), a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 4
POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, 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. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego Załącznik Nr 8 do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, póz. 926 z późniejszymi zmianami) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami), 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).
6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie wchodzi w życie z dniem jej podpisania przez Burmistrza.

Załącznik Nr 1 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:
przetwarzane zgodnie z prawem,
zbierane dla oznaczonych, zgodnych z prawem celów,
merytorycznie poprawne i adekwatne w stosunku do celów.
2. administrator danych wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
3. opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych;
4. określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
5. opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji;
6. prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:
ochronę danych przed niepowołanym dostępem,
nieuzasadnioną modyfikację lub zniszczenie danych,
nielegalne ujawnienie danych.
9. rejestruje zbiory danych osobowych w Biurze Generalnego Inspektora Ochrony Danych Osobowych

Załącznik Nr 2 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Obowiązki Administratora Bezpieczeństwa Informacji

Do obowiązków Administratora Bezpieczeństwa Informacji należy :
nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym,
nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe,
nadzór na wykorzystywanym w Urzędzie oprogramowaniem oraz jego legalnością.
przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe,
podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych,
badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych,
nadzór na naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe,
definiowanie użytkowników i haseł dostępu,
przeprowadzanie symulowanych włamań do systemu w celu ustalenia aktualnego poziomu zabezpieczeń,
aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie,
nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności,
wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych,
sporządzanie planów kontroli zatwierdzanych przez Administratora Danych oraz przeprowadzanie zgodnie z nimi kontroli,
sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Załącznik Nr 3 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Dodatkowy zakres obowiązków
dla pracowników Urzędu Miasta i Gminy w Baranowie Sandomierskim

1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:
chronić dane przed dostępem osób nieupoważnionych,
chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Urzędzie.
archiwizować dane zgodnie z instrukcją technologiczną,
prowadzić niezbędną, przewidzianą instrukcją technologiczną dokumentację pracy z systemem, archiwizowania danych itp.
2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,
kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa,
zabrania się przetwarzania danych w sposób inny niż opisany instrukcją technologiczną.

Załącznik Nr 4 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

..... Baranów Sandomierski, dn. .....
(imię i nazwisko pracownika)

.....
(adres)
.....

OŚWIADCZENIE

(tekst oświadczenia podpisanego przez pracowników Urzędu Miasta i Gminy w Baranowie Sandomierskim oraz służb pomocniczych – sprzątaczka)

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
o ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową,
o zasadach ochrony oraz środkach i zabezpieczeniach danych osobowych (Dz. U. Nr 133 poz. 833) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 28 kwietnia 2004 roku (Dz. U. z 2004 r. Nr 100 poz. 1024.) oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych.
2 Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy w Urzędzie, a w szczególności nie będę:
ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tym systemach,
ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowania,
udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją technologiczną.

....
(podpis pracownika) (podpis przełożonego)

Załącznik Nr 5 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Opis struktur zbiorów danych

Zbiór danych „Ewidencja ludności" zawiera następujące pola:
dane osobowe:
nazwiska i imiona,
nazwisko rodowe i z poprzedniego małżeństwa
imiona rodziców,
data urodzenia,
miejsce urodzenia,
akta urodzenia, data i nr USC;
dane osobowe archiwalne
nazwiska i imiona,
nazwisko rodowe i z poprzedniego małżeństwa
adres zamieszkania lub pobytu stałego oraz data zameldowania;
archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania;
adres czasowy oraz czas pobytu czasowego
archiwalne adresy czasowe oraz okresy pobytów czasowych
dokument tożsamości:
rodzaj dokumentu,
seria i numer dowodu,
wystawca dokumentu,
rysopis: wzrost, kolor oczu, znaki szczególne;
numer ewidencyjny PESEL,
USC i nr aktu urodzenia,
stan cywilny:
imię i nazwisko współmałżonka,
nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
data zawarcia małżeństwa,
USC i numer aktu małżeństwa,
data wydania i wydający dokument tożsamości,
stan cywilny archiwalny:
imię i nazwisko współmałżonka,
nazwisko rodowe i nazwisko z poprzedniego małżeństwa,
data zawarcia małżeństwa,
USC i numer aktu małżeństwa,
data wydania i wydający dokument tożsamości,
archiwalne dokumenty tożsamości,
obowiązek wojskowy:
a). czy podlega obowiązkowi
b). nazwa i nr wojskowego dokumentu tożsamości
c). stopień wojskowy,
15) data zgonu, USC i numer aktu zgonu,
imiona i nazwiska rodowe,
narodowość,
obywatelstwo (data zmiany, podstawa prawna)
adnotacje o rozwodzie.

Zbiór danych „USC i dowody osobiste" zawiera następujące pola:
imiona i nazwiska,
imiona i nazwiska rodowe rodziców,
nazwisko rodowe,
data urodzenia,
miejsce urodzenia,
numer PESEL,
kolor oczu,
wzrost w cm,
płeć,
adres zamieszkania,
rodzaj zameldowania,
kod pocztowy,
posiadany dotychczasowy dokument tożsamości (seria, nr, nazwa i siedziba wystawcy),
przyczyna wystawienia dowodu,
data i przyczyna utraty,
podpis osoby,
fotografia.

Zbiór danych „Podatki" zawiera następujące pola:
imię i nazwisko podatnika,
adres zamieszkania,
numer NIP,
numer PESEL,
numery aktów notarialnych,
numery działek.

Zbiór danych „Świadczenia rodzinne" zawiera następujące pola:
42) dane osobowe:
imię i nazwisko,
data urodzenia,
płeć,
numer NIP,
numer PESEL,
stan cywilny,
numer i seria dowodu osobistego,
numer paszportu,
obywatelstwo,
przynależność do oddziału NFZ (kasa chorych),
nazwa banku i numer konta
43) dane adresowe:
adres zamieszkania (miejscowość, ulica, nr, domu, nr lokalu, kod pocztowy, poczta, nr telefonu),
adres zameldowania (miejscowość, ulica, nr, domu, nr lokalu, kod pocztowy, poczta),
nr telefonu.

Załącznik Nr 6 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Granice obszarów, w których przetwarzane są dane osobowe

§1. Pomieszczeniami tworzącymi obszar, którym znajdują się przetwarzane dane osobowe są pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów i innych oraz stacjonarny sprzęt komputerowy, w którym znajdują się dane osobowe.

§2. W budynku Urzędu obszarem, w którym przetwarzane są dane osobowe w formie kartotek, rejestrów i stacjonarnego sprzętu komputerowego jest pomieszczenie:
pokój nr 2 – parter – obsługa programu „ELUD+", „WYB+" oraz „PB_USC",
pokój nr 3 – parter – obsługa programu „EZAR+","FA+" i"WIP+", Świadczenia Rodzinne,
pokój nr 7 – I piętro – obsługa programów „EGRUN+" , "POGRUN" i „WIP+", Podatki
pokój nr 9 – I piętro - obsługa programu „ESO+" Stypendia szkolne
pokój nr 12 i 13 – I piętro – obsługa programów „FKB+", „PŁACA+", „KADRY+", - Księgowość

Załącznik Nr 7 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Wzór

Raport
z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

1. Data: ..... Godzina: .....
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:
.....
.....
.....

6. Podjęte działania:
.....
.....
.....

7. Postępowanie wyjaśniające:
.....
.....
.....

.....
(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 8 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Baranowie Sandomierskim

Wzór

Wykaz osób,
które zostały zapoznane z „Polityką bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
w Urzędzie Miasta i Gminy w Baranowie Sandomerskim
przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis