Zarządzenie Nr 35/09
Wójta Gminy Naruszewo
z dnia 4 sierpnia 2009 r.

w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych (tj. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 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) zarządzam co następuje:

§ 1

1. Wprowadza się dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie Gminy Naruszewo.
2. Na dokumentację o której mowa w ust. 1 składa się:

a) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Naruszewo stanowiąca załącznik nr 1 do zarządzenia,

b) Polityka bezpieczeństwa zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiąca załącznik nr 2 do zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

mgr inż. Beata Pierścińska

Załącznik nr 1
do Zarządzenia Wójta Gminy
Naruszewo nr 35/09
z dnia 4 sierpnia 2009 roku

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Rozdział I.
CZĘŚĆ
OGÓLNA

§ 1

Instrukcja określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy Naruszewo.

§ 2

Ilekroć w niniejszej instrukcji mowa o:

1. Urzędzie - należy przez to rozumieć Urząd Gminy Naruszewo,
2. Administratorze Danych Osobowych - należy przez to rozumieć Wójta Gminy Naruszewo,
3. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć osobę wyznaczoną przez Administratora Danych Osobowych do pełnienia tej funkcji,
4. Lokalnym Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć Kierownika Referatu lub pracownika zatrudnionego na samodzielnym stanowisku, przewidzianych w strukturze organizacyjnej Urzędu,
5. użytkowniku danych osobowych – należy przez to rozumieć każdego pracownika, który wykonując czynności służbowe przetwarza dane osobowe, tzn. wykonuje na nich jakiekolwiek operacje, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie,
6. systemie informatycznym – należy przez to rozumieć system informatyczny wdrożony w Urzędzie Gminy Naruszewo.

§ 3

Za dane osobowe uznaje się informacje zawarte w prowadzonych w Urzędzie Gminy Naruszewo różnego rodzaju rejestrach, ewidencjach, kartotekach, wykazach oraz w systemach informatycznych dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, pozwalające na bezpośrednie lub pośrednie określenie tożsamości tej osoby.

§ 4

1. Do obowiązków Administratora Bezpieczeństwa Informacji należy:

a) czuwanie nad wdrażaniem w Urzędzie niniejszej instrukcji oraz dbanie o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych,
b) identyfikacja i analiza zagrożeń oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych,
c) określanie potrzeb w zakresie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe,

d) nadawanie identyfikatorów użytkownikom danych osobowych,
e) zabezpieczenie i kontrolowanie prawidłowości przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,
f) pozbawianie zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie urządzeń lub nośników, które przeznaczone są do likwidacji,
g) instalowanie zabezpieczeń w systemach informatycznych,
h) wyrejestrowywanie i rejestrowanie z systemu użytkowników w czasie instalowania oraz modyfikacji systemu,
i) przydzielanie uprawnień do poszczególnych systemów,
j) wykonywanie kopii awaryjnych danych z serwera, właściwe przechowywanie nośników, sprawdzanie poprawności zapisu oraz ich likwidowanie,
k) dokonywanie wyboru lub migracji do technologii minimalizującej zagrożenia uzyskania dostępu do sieci osobom nieupoważnionym,
l) nadzorowanie procesu monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nie upoważnionych,
m) sporządzanie oraz bieżące aktualizowanie listy osób upoważnionych do pobierania kluczy od pomieszczeń, w których przetwarzane są dane osobowe,
n) prowadzenie ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych.

2. Do obowiązków Lokalnego Administratora Bezpieczeństwa Informacji należy:
a) wykonywanie poleceń Administratora Bezpieczeństwa Informacji w zakresie zarządzania podległymi systemami informatycznymi,
b) czuwanie nad właściwym eksploatowaniem podległych im systemów informatycznych,
c) stwarzanie właściwych warunków organizacyjno-technicznych gwarantujących bezpieczeństwo podległych im systemów informatycznych,
d) nadzorowanie właściwej lokalizacji sprzętu komputerowego, tj. ustawiania monitorów i drukarek uniemożliwiającego wgląd w dane osobowe osobom nieupoważnionym lub kradzież wymiennych nośników danych,
e) nadawanie haseł dostępu użytkownikom oraz ustawianie uprawnień w podległych im systemach,
f) pozbawianie zapisu danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych,
g) pozbawianie zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie nośników, które przeznaczone są do likwidacji,
h) prowadzenie, uaktualnianie na bieżąco oraz przesyłanie Administratorowi Bezpieczeństwa Informacji danych dotyczących:
   - ✓ listy użytkowników danych osobowych wraz z przydzielonymi im uprawnieniami do poszczególnych funkcji systemu,
   - ✓ lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku jakichkolwiek zmian tych danych,
   - ✓ rodzaju systemów informatycznych funkcjonujących w zakresie ich działania,
   - ✓ czynności serwisowych wykonywanych w podległych systemach informatycznych,
   - ✓ zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytych wirusów, koni trojańskich itp. oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania,
i) zgłaszanie Administratorowi Bezpieczeństwa Informacji potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych.

§ 5

1. Dostęp pracowników do obsługi systemu informatycznego przetwarzającego dane osobowe oraz urządzeń wchodzących w jego skład możliwy jest wyłącznie na podstawie upoważnienia wydanego przez Administratora Danych Osobowych,
2. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia,
3. Oświadczenia o zachowaniu tajemnicy służbowej, o której mowa w ust. 2 przechowywane są w aktach osobowych pracowników,
4. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych.

§ 6

1. Udostępnianie danych osobowych ze zbioru danych osobom lub podmiotom uprawnionym do ich otrzymania odbywać się może na pisemny umotywowany wniosek,
2. Decyzję o udostępnieniu danych osobowych podejmuje Administrator Danych Osobowych, po uzyskaniu opinii wydziału merytorycznego,
3. Po otrzymaniu zgody od Administratora Danych Osobowych, dane do udostępnienia przygotowuje użytkownik danych osobowych. Użytkownik jest zobowiązany do odnotowania w systemie informatycznym informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.

Rozdział II.
ZASADY PRZYDZIAŁU HASEŁ DLA UŻYTKOWNIKÓW

§ 7

1. Dla każdego użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe przydziela się odrębny identyfikator i hasło oraz uprawnienia w systemie zgodnie z zakresem obowiązków,
2. Przyznany użytkownikom identyfikator jest niezmienny, natomiast użytkownik jest zobowiązany do zmiany hasła raz na miesiąc,
3. Za przydział i rejestrację identyfikatorów dostępu do systemów przetwarzających dane osobowe odpowiedzialny jest Administrator Bezpieczeństwa Informacji,
4. Za przydział i rejestrację haseł dostępu do poszczególnych systemów przetwarzających dane osobowe odpowiedzialny jest Lokalny Administrator Bezpieczeństwa Informacji,
5. Lokalny Administrator Bezpieczeństwa Informacji wyrejestrowuje z podległego mu systemu identyfikator i hasło pracownika, który utracił uprawnienia dostępu do danych osobowych. Administrator Bezpieczeństwa Informacji wyrejestrowuje konto takiego użytkownika w systemie sieciowym,
6. Identyfikatory pracowników oraz hasła dostępu do systemu informatycznego stanowią tajemnicę służbową,
7. Użytkownik po otrzymaniu indywidualnego identyfikatora oraz hasła powinien je zapamiętać. Nie wolno ich zapisywać w miejscach, które umożliwiłyby osobom trzecim zapoznanie się z nimi,
8. W przypadku, gdy dane osobowe przetwarzane są w programach typu Office na pojedynczym komputerze, użytkownik danych osobowych zobowiązany jest zabezpieczyć plik hasłem.

Rozdział III.
PROCEDURY ROZPOCZĘCIA I ZAKOŃCZENIA PRACY PRZY KOMPUTERZE

§ 8

1. Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną,
2. Użytkownicy uzyskują bezpośredni dostęp do danych w aplikacji po podaniu identyfikatora i właściwego hasła,
3. Kończąc pracę użytkownik powinien:

a) wykonać kopię awaryjną (zapasową),
b) zamknąć program oraz wyjść z systemu i wyłączyć komputer wraz z drukarką,
c) sprawdzić, czy pozostawione stanowisko nie stwarza jakichkolwiek zagrożeń i czy są prawidłowo zabezpieczone przed uruchomieniem ich przez osoby postronne,
d) sprawdzić czy w napędach komputera nie pozostały nośniki zawierające dokumenty lub informacje zawierające dane osobowe, niejawne lub inne do których wgląd modą mieć jedynie wybrani pracownicy urzędu.

4. Wszystkie zauważone usterki i mankamenty na stanowisku użytkownik winien natychmiast zgłosić bezpośredniemu przełożonemu oraz Administratorowi Bezpieczeństwa Informacji.

§ 9

1. użytkownik danych osobowych, który stwierdzi naruszenia zabezpieczeń systemu informatycznego, na które mogą wskazywać:

a) stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),
b) różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych opcjach),
c) różnica w zawartości zbioru danych osobowych (np. brak lub nadmiar danych)

zobowiązany jest niezwłocznie powiadomić o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji, a w przypadku ich nieobecności - bezpośrednio Administratora Danych Osobowych.

2. Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba powinna w pierwszej kolejności:

a) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas wykrycia tego faktu,
b) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,
c) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
d) niezwłocznie podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji,
e) przywrócić normalny stan działania systemu.

3. Po wyeliminowaniu bezpośredniego zagrożenia Administrator Bezpieczeństwa Informacji ma obowiązek przeprowadzić analizę stanu systemu informatycznego, a w szczególności sprawdzić:

a) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

b) zawartość zbioru danych osobowych,
c) sposób działania programu,
d) jakość komunikacji w sieci telekomunikacyjnej,
e) obecność wirusów komputerowych.

Rozdział IV
METODY I CZĘSTOTLIWOŚĆ TWORZENIA KOPII AWARYJNYCH ORAZ SPOSÓB I CZAS ICH PRZECHOWYWANIA

§10

1. Dane zgromadzone w pamięciach komputerów powinny być zabezpieczone przed ich utratą przez tworzenie ich kopii awaryjnych w cyklach:
   - codziennym,
   - tygodniowym,
   - miesięcznym.
2. Za archiwizację danych przechowywanych w pamięci komputerów lokalnych odpowiedzialni są użytkownicy danych osobowych. Archiwizacji należy dokonywać w każdym dniu, w którym dokonywane były jakiekolwiek zmiany. Dane powinny być kopiowane na wyznaczony dysk sieciowy, dyskietki 1,44 MB lub płyty CD-R – przechowywane w pomieszczeniu wskazanym przez Lokalnego Administratora Bezpieczeństwa.
3. Za archiwizację danych przechowywanych w pamięci serwerów sieciowych odpowiedzialny jest Administrator Bezpieczeństwa Informacji. W cyklu codziennym należy archiwizować zmiany, a w cyklu tygodniowym całą zawartość baz danych przechowywanych w pamięci serwerów sieciowych. Zarchiwizowane dane należy przechowywać w odpowiednio chronionym i zabezpieczonym pomieszczeniu, poza pomieszczeniem w którym umieszczony jest serwer sieciowy.
4. Kopie zapasowe danych z serwera archiwizowane w cyklu miesięcznym należy przechowywać w odpowiednio zabezpieczonym pomieszczeniu innym niż pomieszczenie w którym przechowywane są dane z cykli codziennych i tygodniowych, poza pomieszczeniem w którym znajduje się serwer. Za archiwizowanie danych z pamięci serwerów w cyklu miesięcznym odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

Rozdział V.
SPOSÓB i CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI

§ 11

1. Nośniki informatyczne, wydruki zawierające dane osobowe oraz kopie awaryjne, o których mowa w § 10 ust. 2-4, przechowywać należy w wyznaczonych pomieszczeniach, w zamkniętych szafach,
2. Kopie zapasowe, o których mowa w § 10 ust. 2 i 3 powinny być przechowywane przynajmniej 7 dni,
3. Kopie zapasowe, o których mowa w § 10 ust. 4 winny być przechowywane przynajmniej przez 6 miesięcy,
4. Użytkownicy na koniec każdego okresu, o którym mowa w ust. 2 i 3, winni dokonać analizy przydatności kopii awaryjnych,
5. Za wydruki zawierające dane osobowe odpowiedzialni są użytkownicy danych osobowych, którzy je wykonali. Wydruki te winny być przechowywane zgodnie

z terminami określonymi w instrukcji kancelaryjnej,

6. Każdy użytkownik ma obowiązek pozbawiania zapisu danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych oraz do pozbawiania zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie nośników, które przeznaczone są do likwidacji.

Rozdział VI.
DOKONYWANIE PRZEGLĄDÓW I KONSERWACJI SYSTEMU I ZBIORU DANYCH OSOBOWYCH

§ 12

1. Raz na kwartał Administrator Bezpieczeństwa Informacji lub wyznaczona przez niego osoba, dokonuje przeglądu i konserwacji systemu informatycznego i zbioru danych osobowych,
2. W przypadku konieczności oddania sprzętu zawierającego dane osobowe do naprawy na zewnątrz, Administrator Bezpieczeństwa Informacji zobowiązany jest do usunięcia zapisanych danych. W przypadku gdy nie można tych danych usunąć, naprawa sprzętu winna być dokonywana pod nadzorem Administratora Bezpieczeństwa Informacji.

Rozdział VII.
SPOSÓB POSTĘPOWANIA W ZAKRESIE ZWIĘKSZENIA BEZPIECZEŃSTWA SIECI KOMPUTEROWEJ

§ 13

1. Ogranicza się w Urzędzie obieg dyskietek i innych nośników informatycznych poprzez ich ostemplowanie pieczęcią Urzędu Gminy Naruszewo,
2. Wprowadza się zakaz obiegu nośników nie oznakowanych w sposób, o którym mowa w ust. 1, a wszystkie nośniki przychodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu z nich danych po uprzednim sprawdzeniu programem antywirusowym u informatyków Urzędu.

§ 14

Systemy do przetwarzania danych osobowych są zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu, przez odpowiednie oprogramowanie.

§ 15

Zabrania się:

1. udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,
2. wykorzystywania sieci komputerowej w celach innych niż służbowych,
3. samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji),
4. trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie,
5. publicznego rozpowszechniania programów komputerowych lub ich kopii,
6. przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
7. udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu,
8. wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego

rozpowszechniania bez wyraźnego upoważnienia Administratora Bezpieczeństwa Informacji,

9. używania prywatnych skrzynek mailowych działających na innych serwerach bez uzgodnienia z Administratorem Bezpieczeństwa Informacji,
10. uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści,
11. kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody Administratora Danych Osobowych.

Wójt

mgr inż. Beata Pierścińska

Załącznik nr 2
do Zarządzenia Wójta Gminy
Naruszewo Nr 35/09
z dnia 4 sierpnia 2009 r.

Polityka bezpieczeństwa.

1. Wykaz budynków i pomieszczeń Urzędu tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego

Budynek Urzędu Gminy Naruszewo

Lp.	Numer pomieszczenia	Nazwa Wydziału, nazwa pomieszczenia
1	6, 8, 4	Referat Społeczno Gospodarczy
2	5	samodzielne stanowisko ds. obronnych, obrony cywilnej, zarządzania kryzysowego i kadr
3	2, 3, 7	Referat Organizacyjny i Spraw Obywatelskich
4	13, 14, 15	Referat Finansowy
5	7	Urząd Stanu Cywilnego

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru danych osobowych	Nazwa programu zastosowanego do ich przetwarzania
1	Podatek Rolny / Nieruchomości	PR i PN
2	Program Kadrowo Płacowy	KDiP
3	Rozliczenia ZUS	Płatnik
4	Ewidencja Ludności	SELWIN
5	Urząd Stanu Cywilnego	USCWIN
6	Ewidencja Gruntów i Budynków	EWOPIS

3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

a) Moduły sytemu *Podatek Rolny / Nieruchomości* przechowywane są na komputerze pełniącym rolę zarówno serwera dla programu *PR i PN* jak i stacji roboczej pracującej w oparciu o MS WINDOWS XP. Dostęp do danych przyznawany jest na podstawie utworzonych w systemie kont użytkowników. Jedynie pracownicy odpowiadający za przetwarzanie tych danych posiadają konta umożliwiające dostęp do bazy.

b) Moduły sytemu *Program Kadrowo Płacowy* przechowywane są na komputerze pełniącym

rolę zarówno serwera dla programu *KDiP* jak i stacji roboczej pracującej w oparciu o MS WINDOWS XP. Dostęp do danych przyznawany jest na podstawie utworzonych w systemie kont użytkowników. Jedynie pracownicy odpowiadający za przetwarzanie tych danych posiadają konta umożliwiające dostęp do bazy.

c) Moduły sytemu *Rozliczenia ZUS* przechowywane są na komputerze pełniącym rolę zarówno serwera dla programu *Płatnik* jak i stacji roboczej pracującej w oparciu o MS WINDOWS XP. Dostęp do danych przyznawany jest na podstawie utworzonych w systemie kont użytkowników. Jedynie pracownicy odpowiadający za przetwarzanie tych danych posiadają konta umożliwiające dostęp do bazy.

d) Moduły sytemu *Ewidencja Ludności* przechowywane są na komputerze pełniącym rolę zarówno serwera dla programu *SELWIN* jak i stacji roboczej pracującej w oparciu o MS WINDOWS XP. Dostęp do danych przyznawany jest na podstawie utworzonych w systemie kont użytkowników. Jedynie pracownicy odpowiadający za przetwarzanie tych danych posiadają konta umożliwiające dostęp do bazy.

e) Moduły sytemu *Urząd Stanu Cywilnego* przechowywane są na komputerze pełniącym rolę zarówno serwera dla programu *USCWIN* jak i stacji roboczej pracującej w oparciu o MS WINDOWS XP. Dostęp do danych przyznawany jest na podstawie utworzonych w systemie kont użytkowników. Jedynie pracownicy odpowiadający za przetwarzanie tych danych posiadają konta umożliwiające dostęp do bazy.

f) Moduły sytemu *Ewidencja Gruntów i Budynków* przechowywane są na komputerze pełniącym rolę zarówno serwera dla programu *EWOPIS* jak i stacji roboczej pracującej w oparciu o MS WINDOWS XP. Dostęp do danych przyznawany jest na podstawie utworzonych w systemie kont użytkowników. Jedynie pracownicy odpowiadający za przetwarzanie tych danych posiadają konta umożliwiające dostęp do bazy.

4. Sposób przepływu danych pomiędzy poszczególnymi systemami.

W Urzędzie systemy: *PR i PN*, *KDiP*, *Płatnik*, *SELWIN*, *USCWIN*, *EWOPIS* są współdzielone sieciowo miedzy wielu użytkowników, każdy z niech korzysta ze wspólnej wydzielonej dla siebie baz danych, znajdującej się w tym samym folderze. Dostęp do danych jest współdzielony i każdy z systemów: *PR i PN*, *KDiP*, *Płatnik*, *SELWIN*, *USCWIN*, korzysta z danych w określonym dla siebie zakresie. Systemy te nie współpracują między sobą i nie ma między nimi przepływu danych.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Wszystkie programy wykorzystywane do przetwarzania danych osobowych posiadają własny system identyfikacji użytkowników. Każdy użytkownik przetwarzający dane osobowe posiada swój własny identyfikator utworzony w programie, w którym przetwarza dane. Identyfikator taki zabezpiecza dane przed niepowołanym dostępem. Poszczególne systemy za pomocą mechanizmu rejestracji zapamiętują informacje związane z czasem pracy użytkowników. Pracownicy Urzędu mają przydzielone zakresy obowiązków zgodnie, z którymi odpowiadają za przetwarzanie określonych baz danych osobowych. W każdym przypadku jest wyznaczona jedna osoba (oraz osoby zastępujące ją na czas nieobecności) odpowiedzialna za konkretny zbiór danych, posiadająca niepowtarzalny identyfikator, który umożliwia rozliczalność wprowadzanych zmian.

Wójt

mgr inż. Beata Pierścińska