Załącznik nr 2
do zarządzenia nr 117/2008

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

§ 1

Cel wydania dokumentu:

Realizacja postanowień Zarządzenia Wójta Gminy Osięciny nr 117/2008 z dnia 15 lutego 2008 r. w sprawie ustalenia polityki bezpieczeństwa przetwarzania danych osobowych systemu informatycznego w Urzędzie Gminy w Osięcinach oraz postanowień § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r 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).

Rozdział I

Postanowienia ogólne

§ 2

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy zwana dalej" instrukcją" określa:

1. Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym urzędu (rozdział II).
2. Metody i środki uwierzytelnienia w systemie informatycznym oraz procedury związane z ich zarządzaniem i użytkowaniem (rozdział III).
3. Procedury rozpoczęcia, zawieszenie i zakończenia pracy w systemie (rozdział IV).
4. Procedury tworzenia kopii zapasowych zbiorów zarejestrowanych u Generalnego Inspektora Ochrony Danych Osobowych oraz programów i narzędzi programowych

służących do jego przetwarzania (rozdział V).

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe (rozdział VI).

6. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi (rozdział VII).

7. Zasady i sposób odnotowywania w systemie informacji: komu, kiedy i w jakim zakresie dane osobowe ze zbiorów zostały udostępnione (rozdział VIII).

8. Procedury wykonania przeglądów i konserwacji systemu, w tym elektronicznych nośników informacji służących do przetwarzania danych osobowych (rozdział IX).

9. Przetwarzanie danych osobowych w zbiorach doraźnych. (rozdział X).

10. Sposób przepływu danych poniędzy poszczególnymi systemami informacyjnymi w sieci lokalnej w Urzędzie Gminy w Osięcinach – załącznik nr 2.

11. Informację o sprzęcie komputerowym na stanowisku roboczym określa karta ewidencji zestawu komputerowego – załącznik nr 3.

12. Informację o zainstalowanym oprogramowaniu na stanowisku roboczym określa karta oprogramowania – załącznik nr 4.

§ 3

Definicje

Ilekroć mowa w niniejszym dokumencie o:

a) Urząd - należy przez to rozumieć Urząd Gminy w Osięcinach

b) Administrator Danych Osobowych - (zgodnie z ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997r (Dz. U. z 2002r Nr 101, poz. 926 z późn. zm.) - Wójt Gminy.

c) Administrator Bezpieczeństwa Informacji (ABI) - należy przez to rozumieć pracownika urzędu wyznaczonego przez Wójta do nadzorowania przestrzegania zasad ochrony określonych w Zarządzeniu Wójta Gminy w Osięcinach Nr. 117/2008 z dnia 15 stycznia 2008r. w sprawie przetwarzania danych osobowych w systemie informatycznym urzędu oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,

d) użytkowniku systemu - należy przez to rozumieć osobę upoważnioną przez ADO (Wójt Gminy) do przetwarzania danych osobowych w systemie informatycznym i ręcznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu.

e) sieci lokalnej - należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie do własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

f) telekomunikacyjnej sieci rozległej - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000r - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)

§ 4

Rozdział II

Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym Urzędu Gminy.

l. Podstawowe zasady nadawania uprawnień w systemie informatycznym Urzędu Gminy

a) Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się: z ustawą z dnia 29 sierpnia 1997r o ochronie danych osobowych (Dz. U. z 2002r Nr 101, poz. 926 z późn. zm.), oraz Zarządzeniem Wójta Gminy Osięciny Nr 117/2008 w sprawie przetwarzania danych osobowych w urzędzie, dokumentem określającym podstawowe zagrożenia związane z przetwarzaniem danych osobowych w systemie informatycznym oraz zastosowane w celu ochrony danych osobowych środki techniczne i organizacyjne;

b) Jedynie użytkownik zobowiązany jest do wypełnienia wniosku o nadanie uprawnień w systemie informatycznym oraz dokonuje zmian tych uprawnień w systemie – załącznik nr. 5.

2. Procedura nadawania uprawnień do przetwarzania danych osobowych

Upoważnienie do przetwarzania danych osobowych nadaje - administrator danych osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych,

ABI wypełnia upoważnienie dla danej osoby, oraz sporządza aneks do zakresu czynności, które zostają podpisane przez Administratora Danych Osobowych (Wójta), następnie zarejestrowane i przekazane do akt osobowych danego pracownika.
ABI wypełnia wyrejestrowane użytkownika, oraz sporządza aneks do zakresu czynności, które zostają podpisane przez (Wójta), następnie zarejestrowane i przekazane do akt osobowych danego pracownika.
Upoważnienie jako załącznik nr. 1 do niniejszej instrukcji.

§ 5

Rozdział III

Metody i środki uwierzytelnienia w systemie informatycznym urzędu oraz procedury związane z ich zarządzaniem i użytkowaniem

A. Metody i środki uwierzytelnienia
1. W systemie informatycznym urzędu stosuje się uwierzytelnienia dwustopniowe na poziomie:
a) dostępu do sieci lokalnej;
b) dostępu do aplikacji.
2. Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła.
3. Hasło na poziomie dostępu do aplikacji składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
4. Hasło dostępu do sieci lokalnej składa się co najmniej z 6 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
5. Hasło, o którym mowa w pkt. 4 nie może być powtórnie użyte.
6. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat. imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
7. Hasło nie może być ujawnione nawet po utracie przez nie ważności.

8. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

9. Hasło przekazywane jest w kopercie za potwierdzeniem przekazania ABI.

10. Zmiana hasła następuje w pierwszym dniu następnego miesiąca w ciągu 1 godziny od chwili ustalenia nowego hasła.

B. Procedury zarządzania środkami uwierzytelnienia

l. ABI nadaje hasło dostępu do aplikacji dla nowego użytkownika albo dla użytkownika, który zapomniał swojego ostatniego hasła.

2. Użytkownik systemu niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ABI.

3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu po ustaleniu z ABI.

4. Użytkownik systemu zapisuje swój identyfikator i hasła dostępu do aplikacji i przekazuje je w kopercie ABI. Koperta zostaje zabezpieczona w sposób uniemożliwiający jej nieuważne otwarcie. ABI przechowuje kopertę w szafie w pokoju 20.

§ 6

Rozdział IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

A. Procedura rozpoczęcia pracy.

1.Uruchomić komputer wchodzący w skład systemu informatycznego gminy, podłączony fizycznie do sieci lokalnej i załogować się do sieci podając swój identyfikator i hasło dostępu do sieci.

2. Uruchomić aplikację systemu, podając następnie swój identyfikator i hasło dostępu do aplikacji.

3. Rozpocząć pracę.

B. Procedura zawieszenia pracy w systemie.

1. W trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego, sprawdzić ekran czy nie są wyświetlane dane osobowe.

2. Przy opuszczeniu pokoju na dłuższy czas (tzn. 2 minuty) ustawić bezwzględnie wygaszasz ekranu z hasłem zabezpieczającym wygaszacz.

C. Procedura zakończenia pracy w systemie.

l. Zamknąć aplikację

2. Zamknąć system.

3. Wyłączyć monitor i drukarkę.

§ 7

Rozdział V

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do jego przetwarzania.

1 Kopię bezpieczeństwa wykonuje w cyklu miesięcznym:

- Ochrona Środowiska,
- Kadry
- Świadczenia Rodzinne,
- Stypendia Socjalne,
- Ewidencja ludności,
- Ewidencja działalności gospodarczej,
- Gminny Ośrodek Pomocy Społecznej
- Zespól Szkół i Placówek Oświatowych,
- Księgowość,
- Podatki.

2. ABI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

3. Serwer ustawiony w ten sposób, aby kopie dzienne zapisywane były na dyskach z obsługą RAID.

4. Kopie z serwera wykonywane są co dwa tygodnie, nagrywane na nośniki zewnętrzne (PENDRIVE).

§ 8

Rozdział VI

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

A. Elektroniczne nośniki informacji zawierające dane osobowe.

1. Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym urzędu, zapisane na nośnikach magnetycznych nie są wynoszone poza siedzibę urzędu.

2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych.

3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub metalowych.

4. Dane osobowe w postaci elektronicznej należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtwarzanie, nie później niż po upływie 3 dni, po wykorzystaniu tych danych chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

5. Nośniki magnetyczne z danymi osobowymi należy niszczyć zgodnie z obowiązującymi w gminie przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi.

6. Kasacji nośników nieprzydatnych wykonuje się na odpowiedniej niszczarce do płyt.

7. Dyski twarde podlegają komisyjnemu zniszczeniu w pokoju nr 20. W skład tej komisji wchodzi Wójt, Sekretarz oraz ABI.

B. Kopie zapasowe

1. Kopie zapasowe zbiorów danych do przetwarzania danych osobowych są przechowywane w pokoju nr 20 w szafach.

2. Dostęp do niej mają tylko upoważnieni pracownicy.

C. Wydruki

l. Wydruki zawierające dane osobowe, należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych.

2. Wydruki zawierające dane osobowe, należy zniszczyć przez pocięcie w specjalnym urządzeniu nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

§ 9

Rozdział VII

Środki ochrony systemu przed wprowadzeniem danych oprogramowania, w tym wirusami komputerowymi

A. Ochrona antywirusowa

1. Za ochronę antywirusową odpowiada ABI.

2. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje ABI wykorzystując w trakcie pracy systemu informatycznego moduł programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasady systemu informatycznego.

3. Użytkownik systemu na stanowisku komputerowym, importującym dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

B. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej.

1. ABI jest odpowiedzialny za aktywowanie oprogramowania monitorującego wymianę danych (z chwilą uruchomienia tegoż oprogramowania w urzędzie):

a) sieci lokalnej

b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

2. Użytkownicy systemu obowiązani są do utrzymywania stałej aktywności zainstalowanego na ich stanowiskach komputerowych specjalistycznego oprogramowania monitorującego wymianę danych na styku tego stanowiska i sieci lokalnej.

§ 10

Rozdział VIII

Zasady i sposób odnotowywania w systemie informacji o udostępnienie danych osobowych.

1. W systemie informatycznym tego systemu.

2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie Gminy,

c) przedstawiciela, o którym mowa w art. 31 a ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych,

d) podmiotu, któremu powierzono przetwarzanie danych,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem na podstawie odrębnych przepisów.

3. Odnotowanie obejmuje informacje o:

a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,

b) zakresie udostępnianych danych z podaniem podstawy prawnej,

c) dacie udostępnienia.

4. Obowiązek odnotowania w/w informacji spoczywa na użytkowniku systemu

5. Odnotowanie informacji powinno następować niezwłocznie po udostępnieniu danych

6. Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych

7. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje ABI.

§ 11

Rozdział IX

Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych osobowych.

O przeprowadzonych przeglądach i konserwacjach systemu oraz nośników służących do przetwarzania danych osobowych w każdym przypadku informowany jest ABI.

A. Przeglądy i konserwacja urządzeń.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producentów sprzętu.
2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić ABI.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ABI

B. Przegląd programów i narzędzi programowych.

1. Przegląd programów i narzędzi programowych przeprowadzany jest w następujących przypadkach:

a) zmiany wersji oprogramowania serwera plików,

b) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu,

c) zmiany systemu operacyjnego serwera plików,

d) zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu

e) wykonania zmian w projekcie systemu spowodowanych konieczności naprawy, konserwacji lub modyfikacji systemu

2. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmiennej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:

1. poprawność logowania się do systemu w zależności od posiadanych uprawnień
2. poprawność działania wszystkich elementów aplikacji
3. poprawność funkcjonalną systemu symulując działania wszystkich grup użytkowników wykonując następujące operacje:
    a) wprowadzenie danych osobowych
    b) edytowanie danych osobowych
    c) wyszukiwania danych osobowych
    d) wydruku danych osobowych.

C. Konserwacja oprogramowania

1. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.

2. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmiennej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.

§ 12

Rozdział X

Przetwarzanie danych osobowych w zbiorach doraźnych

1. Dostęp do danych osobowych powinien odbywać się poprzez aplikację systemu informatycznego Urzędu. Gdy zachodzi potrzeba zapisania danych w innym formacie np. dane w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione tj.

a) uniemożliwi się dostęp do danych osobowych osobom nieuprawnionym,

b) uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,

c) zabezpieczy się bezpośredni dostęp do danych hasłem.

2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych.

3. Zawiadomić ABI w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.

Wójt Gminy
mgr Jan[illegible] Izydorski