Załącznik Nr 2
do Zarządzenia Nr 155/2010
Wójta Gminy Kotlin
z dnia 4 listopada 2010r.

INSTRUKCJA ZARZĄDZANIA
systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Kotlin

I. Podstawa prawna:

Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych
(tekst jednolity: Dz.U. Nr 101, poz. 926 z 2002r. ze zm.)

Rozporządzenie MSWiA 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)

II. Wprowadzenie:

Celem Instrukcji Zarządzania Systemem Informatycznym jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Kotlin oraz minimalizowanie incydentów mogących zagrozić bezpieczeństwu systemu.

1. Administratorem Danych Osobowych w Urzędzie Gminy Kotlin jest Wójt Gminy Kotlin.
2. Administratorem Bezpieczeństwa Informacji jest osoba nadzorująca z upoważnienia Administratora Danych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych na terenie Urzędu Gminy Kotlin.
3. Administratorem Systemu Informatycznego jest osoba odpowiedzialna za funkcjonowanie systemu, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w systemie.
4. Użytkownikiem systemu jest osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w urzędzie, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż.
5. Sieć lokalna to połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych
6. Sieć publiczna to sieć telekomunikacyjna służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (DZ.U. z 2000r. Nr 73, poz. 852, z późn.zm.)
7. Dane osobowe to wszystkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
8. Zbiór danych to każdy posiadający strukturę zestaw danych o charakterze osobowym.
9. Wykaz zbiorów danych osobowych to wykaz zarejestrowanych jak i nie podlegających rejestracji zbiorów danych osobowych.

10. Przetwarzanie danych to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
11. System informatyczny to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
12. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zwana dalej „instrukcją", jest wewnętrznym dokumentem administratora danych osobowych Urzędu Gminy w Kotlinie, skierowanym do osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym.
13. Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemach informatycznych bez względu na zajmowane stanowisko, miejsce pracy oraz charakter stosunku pracy są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej instrukcji.
14. Polecenia osób wyznaczonych przez administratora danych osobowych do realizacji zadań w zakresie ochrony informacji i bezpieczeństwa systemów informatycznych muszą być bezwzględnie wykonywane przez wszystkich użytkowników.
15. Administrator danych zobowiązuje podwładnych do przestrzegania postanowień tej instrukcji.

III. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych w systemie informatycznym:

1. *Administrator Danych Osobowych* prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym, zawierającą imię, nazwisko, datę nadania uprawnień, datę ustania uprawnień oraz zakres dostępu.
2. *Administrator Bezpieczeństwa Informacji* ustala poziom zabezpieczeń obowiązujących w sieci informatycznej i systemach informatycznych.
3. Systemy informatyczne działające w Urzędzie Gminy w Kotlinie mogą być używane tylko na potrzeby realizacji zadań nałożonych na Urząd Gminy w Kotlinie.
4. Dostęp do sieci informatycznej, systemów informatycznych i programów zabezpieczony jest systemem użytkowników i haseł oraz ograniczeniem dostępu do zasobów sieci. Identyfikator i hasło jednoznacznie identyfikują, weryfikują i autoryzują tożsamość użytkownika.
5. Rejestracji użytkowników w systemie dokonuje *Administrator Systemu Informatycznego* w porozumieniu z Administratorem Bezpieczeństwa Informacji.
6. W systemie informatycznym rejestrowani mogą być wyłącznie użytkownicy, których Administrator Danych Osobowych wpisał do ewidencji osób upoważnionych do przetwarzania danych.
7. W systemach informatycznych dla każdego użytkownika osobno w każdym programie rejestrowany jest odrębny identyfikator powiązany ze znanym tylko i wyłącznie użytkownikowi hasłem. Identyfikator jednoznacznie identyfikuje, weryfikuje i autoryzuje tożsamość użytkownika, a w szczególności jest podstawą do monitorowania czynności użytkownika w systemie oraz dochodzenia konsekwencji tych czynności.
8. Użytkownikom nadawane są uprawnienia do pracy tylko w wymaganych dla realizacji powierzonych zadań modułach i funkcjach programów. Przyznanie, zmiana lub ograniczenie uprawnień następuje na wniosek przełożonego użytkownika złożony Administratorowi Bezpieczeństwa Informacji i jest realizowane przez Administratora Systemu Informatycznego.

9. Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania danych osobowych obliguje Administratora Bezpieczeństwa Informacji w porozumieniu z Administratorem Systemu Informatycznego do odebrania temu użytkownikowi dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz do wyrejestrowania go ze wszystkich systemów informatycznych, do których miał uprawnienia.
10. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie jest usuwany z systemu informatycznego i nie jest przydzielany innej osobie.
11. Administrator Systemu Informatycznego w każdym momencie musi dysponować wykazem identyfikatorów przyznanych użytkownikom w poszczególnych systemach informatycznych powiązanym z imiennym wskazaniem użytkownika danego identyfikatora. Wykaz ten musi uwzględniać również użytkowników, którym odebrano uprawnienia i wyrejestrowano z systemu.

IV. Zasady ustalania i posługiwania się hasłami:

1. Użytkownik jest odpowiedzialny za swoje hasło, w tym za jego okresową zmianę i utrzymywanie w tajemnicy.
2. Użytkownik jest odpowiedzialny za dostosowanie hasła do opisanych niżej reguł, jeśli przestrzegania tych reguł nie wymusza w sposób automatyczny system informatyczny lub oprogramowanie.
3. Żaden z użytkowników, łącznie z Administratorami, nie może mieć możliwości uzyskania z systemu informatycznego aktualnego lub nieważnego hasła innego użytkownika.
4. Administrator Systemu Informatycznego musi mieć możliwość zmiany hasła użytkownika bez znajomości aktualnego lub nieważnego hasła użytkownika.
5. Hasło użytkownika nie może być takie samo jak identyfikator użytkownika.
6. Hasło użytkownika musi składać się z co najmniej 8 znaków, wskazane jest by zawierało litery, cyfry i znaki specjalne.
7. Hasło użytkownika musi być zmieniane nie rzadziej niż co 30 dni. Hasło użytkownika musi być zmienione niezwłocznie w przypadku jego ujawnienia lub podejrzenia ujawnienia.
8. Użytkownik jest zobowiązany do utrzymania swoich haseł w tajemnicy, również po utracie ich ważności.
9. Hasło przy wpisywaniu nie może być w sposób jawny wyświetlane na ekranie.

V. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie:

1. Przed rozpoczęciem pracy w sieci informatycznej użytkownik musi się w niej autoryzować przez podanie swojego identyfikatora i hasła. Dopiero po pomyślnej autoryzacji w sieci informatycznej użytkownik może uruchomić program służący do przetwarzania danych osobowych.
2. Sposób wymiany i przesyłania danych w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników oraz ich działań przy wykorzystaniu sieci informatycznej i oprogramowania.
3. Informacje pozyskane w wyniku monitorowania działań użytkowników oraz pracy urządzeń są dostępne wyłącznie Administratorowi Danych Osobowych, Administratorowi Bezpieczeństwa Informacji i Administratorowi Systemu Informatycznego i mogą być wykorzystane wyłącznie do celów służbowych, związanych z bezpieczeństwem przetwarzania danych w systemach informatycznych.
4. Kontrola przetwarzanych danych prowadzona jest na bieżąco przez użytkownika na każdym stanowisku merytorycznym.

5. W przypadku konieczności czasowego opuszczenia stanowiska pracy użytkownik powinien:
    a) wylogować się z programu lub sieci informatycznej,
    b) zablokować stację roboczą, przy czym odblokowanie może nastąpić dopiero po podaniu hasła
    c) uruchomić wygaszacz ekranu chroniony hasłem.
6. Użytkownik jest zobowiązany do zadbania, aby niemożliwe było odczytanie informacji z monitora przez osoby nieuprawnione.
7. Użytkownik jest zobowiązany do wyrejestrowania się ze systemu informatycznego przed wyłączeniem stacji roboczej.
8. W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu, użytkownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.

VI. Procedury tworzenia kopii zapasowych zbiorów danych:

1. Kopią zapasową i awaryjną objęte są dane znajdujące się na serwerach sieci informatycznej.
2. Za sporządzenie i bezpieczeństwo kopii zapasowych i awaryjnych odpowiedzialny jest Administrator Systemu Informatycznego.
3. Kopia zapasowa wykonywana jest przez kopiowanie całości danych.
4. Harmonogram sporządzania kopii zapasowych musi gwarantować ich dostępność w każdej chwili.
5. Kopie awaryjne tworzone są przed każdą aktualizacją systemu informatycznego, składników systemu informatycznego lub poszczególnych programów służących do przesyłania lub przetwarzania danych. Kopie awaryjne zapisywane są na lokalnym dysku twardym komputera znajdującego się pod stałym nadzorem Administratora Systemy Informatycznego.
6. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych, przy jednoczesnym obowiązku dopilnowania aby dane na lokalnym dysku twardym nie zawierały danych osobowych.
7. W czasie wykonywania kopii zapasowej dostęp do kopiowanych danych dla wszystkich użytkowników jest zablokowany.
8. Po wykonaniu kopii zapasowej i awaryjnej Administrator Systemu Informatycznego ma obowiązek sprawdzić poprawność i kompletność skopiowanych danych oraz zweryfikować możliwość ich przywrócenia i wykorzystania.

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

1. Elektroniczne nośniki informacji
    a) Dane osobowe w postaci elektronicznej zapisane na dyskietkach, dyskach twardych nie można wynosić poza siedzibę urzędu.
    b) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych (określony w Polityce Bezpieczeństwa Danych Osobowych Urzędu Gminy Kotlin).
    c) Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane wyłącznie w zamykanych szafach biurowych.

d) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych.
e) Urządzenia, dyski lub inne nośniki informatyczne zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych. W przypadku, gdy jest to możliwe uszkadza się je w sposób uniemożliwiający ich odczytanie.
f) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Wydruki
   a) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym dostęp osobom nieuprawnionym.
   b) Pomieszczenie, w którym przechowywane są wydruki musi być zamknięte na klucz po godzinach pracy urzędu.
   c) wydruki zawierające dane osobowe w momencie przekazania do usunięcia są niszczone w sposób uniemożliwiający ich odczytanie (w specjalnej niszczarce do papieru)

VIII. Sposób zabezpieczenia systemu informatycznego:

1. System informatyczny jest zabezpieczany przez zastosowanie rozwiązań sprzętowych i programowych.
2. Za aktualność stosowanych zabezpieczeń, dostosowanie do aktualnych potrzeb, konfigurację i zarządzanie nimi odpowiada Administrator Systemu Informatycznego.
3. Administrator Systemu Informatycznego ma obowiązek zgłaszać na piśmie Administratorowi Danych Osobowych wszelkie potrzeby lub zauważone niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.
4. Każdy komputer służący do przetwarzania danych osobowych jest wyposażony w działający cały czas program antywirusowy.
5. Zabrania się stosowania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Za skanowanie odpowiedzialny jest użytkownik komputera.
6. Poczta elektroniczna jest automatycznie sprawdzana przez skaner antywirusowy.