WÓJT GMINY
w Ciechocinie
woj. kujawsko-pomorskie

ZARZĄDZENIE Nr 27/08
WÓJTA GMINY CIECHOCIN
z dnia 20 czerwca 2008

w sprawie dokumentacji dotyczącej przetwarzania danych osobowych w Urzędzie Gminy Ciechocin.

Na podstawie §4 i §5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1. Wprowadzam w Urzędzie Gminy Ciechocin:
1) Instrukcję określającą politykę bezpieczeństwa związaną z przetwarzaniem danych osobowych w Urzędzie Gminy Ciechocin stanowiącą załącznik nr 1 do zarządzenia
2) Instrukcję zarządzania systemem informatycznym Urzędu Gminy Ciechocin stanowiącą załącznik nr 2 do zarządzenia
3) Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych stanowiącą załącznik nr 3 do zarządzenia

§ 2. Traci moc Zarządzenie Nr 31/2006 Wójta Gminy Ciechocin z dnia 19 października 2006 r. w sprawie ustalenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Ciechocin.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr inż. Jerzy Ciszyński

Załącznik Nr 1
do zarządzenia Nr 27/08
Wójta Gminy Ciechocin
z dnia 20 czerwca 2008

Instrukcja
określająca politykę bezpieczeństwa związaną z przetwarzaniem danych osobowych w Urzędzie Gminy Ciechocin

I. Informacje ogólne

1. Definicje
   a) Dane osobowe są to wszelkie dane dotyczące osoby fizycznej i pozwalające na określenie jej tożsamości. Nie uważa się za dane osobowe danych osób zmarłych i danych o osobach prawnych.
   b) Zbiorem danych osobowych jest każdy posiadający strukturę zestaw danych osobowych dostępny według określonych kryteriów systematycznych.
   c) Przetwarzanie danych to wszelkie operacje wykonywane na danych i ich zbiorach, a w szczególności zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
   d) System informatyczny - to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
2. Przedmiotem ochrony są:
   a) zasoby informacyjne (dane) zawierające dane osobowe przechowywane w urzędzie Gminy Ciechocin, ich poufność i autentyczność, a w szczególności ochrona praw osób fizycznych do swobodnego dysponowania własnymi danymi osobowymi,
   b) zasoby informatyczne w tym:
      - struktury i egzemplarze baz danych,
      - standardy administracyjne dotyczące systemów informatycznych związanych z przetwarzaniem baz danych,
      - obiekty materialne oraz ich używanie.
3. Celem polityki bezpieczeństwa danych osobowych jest:
   a) zapewnienie ochrony danych osobowych, z równoczesną możliwością łatwego dostępu do nich przez osoby upoważnione.
   b) przeciwdziałanie realnym i identyfikowalnym zagrożeniom bezpieczeństwa danych osobowych,
   c) wdrożenie i realizacja określonych procedur przetwarzania, przechowywania i udostępniania danych osobowych,
4. Polityka bezpieczeństwa danych osobowych obejmuje:
   a) ograniczenie dostępu do stref przetwarzania danych osobowych,
   b) utrzymywanie wśród pracowników wysokiej świadomości bezpieczeństwa danych osobowych,
   c) monitorowanie stanowisk pracy przetwarzania danych osobowych,
   d) ograniczenie wpływu niepożądanych czynników zewnętrznych, mogących mieć znaczenie dla bezpieczeństwa danych osobowych.
5. Na politykę bezpieczeństwa danych osobowych składają się:
   a) identyfikowanie i analizowanie zagrożeń oraz ocena ryzyka ich wystąpienia,
   b) działania dla zabezpieczenia danych osobowych przed zidentyfikowanymi i potencjalnymi zagrożeniami,
   c) realizacja zabezpieczeń odpowiednich do zagrożeń i uzgodnionych z administratorem (właścicielem) danych osobowych,
   d) monitorowanie działania systemu zabezpieczeń,
   e) prowadzenie szkoleń instruktorów,
   f) prowadzenie dokumentacji dotyczącej ewidencji systemów i istotnych czynności administracyjnych wykonywanych w systemach informatycznych oraz innych czynności związanych z obsługą zasobów informacyjnych i informatycznych zawierających dane osobowe,
   g) określenie sposobów reakcji w przypadku naruszenia polityki bezpieczeństwa.

6. Sprawy dotyczące bezpieczeństwa danych osobowych w urzędzie Gminy Ciechocin prowadzi powoływany przez Wójta Gminy administrator bezpieczeństwa informacji (ABI). Administrator sprawuje nadzór nad zachowaniem zasad polityki bezpieczeństwa określonych niniejszym rozporządzeniem i realizacją przepisów dotyczących ochrony danych osobowych, podejmuje lub inicjuje działania mające na celu przestrzeganie ochrony danych osobowych.

II. Obszar bezpieczeństwa

1) Za obszar, w którym są przetwarzane dane osobowe uznaje się pomieszczenia nr 1, 2, 3, 4, 5, 7, 9 znajdujące się w budynku Urzędu Gminy Ciechocin stanowią obszar przetwarzania danych osobowych.
2) Przebywanie osób nieuprawnionych do dostępu do danych osobowych wewnątrz obszaru przetwarzania danych osobowych jest dopuszczalne tylko w obecności pracownika wskazanego w § 4 ust. 1 i za zgodą administratora bezpieczeństwa informacji lub innej upoważnionej przez niego osoby.
3) Pomieszczenia określone w ust. 1 powinny być zamykane na czas nieobecności w nich pracowników.

III. Wykaz zbiorów danych osobowych

A. Zbiory danych osobowych przetwarzanych przez systemy informatyczne:

1/ Baza danych Programu Finansowo – Księgowego „FOKA"
2/ Baza danych programu „Płatnik"
3/ Baza danych programu „Pomoc materialna"
4/ Baza danych programu „Ewidencja Ludności"
5/ Baza danych programu „Vulcan – Płace"
6/ Baza danych programu „Podatki"
7/ Baza programu „SWDO"
8/ Baza danych programu „Ewidencja Działalności Gospodarczej"

B. Zbiory danych osobowych przetwarzanych bez użycia systemów informatycznych:

8/ Rejestr skarg i wniosków
9/ Rejestr czytelników
10/ Rejestr zamówień publicznych
11/ Rejestr decyzji o warunkach zabudowy i zagospodarowania terenu

IV. Opis struktury zbiorów

Opis zbiorów danych osobowych stanowi odrębny dokument, w którym zawarte są takie dane jak:
- nazwa zbioru
- opis zbioru
- pola informacyjne
- opis powiązań pól informacyjnych
- miejsce przetwarzania formy papierowej
- miejsce przetwarzania formy elektronicznej
- nazwę programu obsługującego formę elektroniczną zbioru danych osobowych

V. Sposób przepływu pomiędzy systemami

Pomiędzy systemami nie następuje przepływ danych osobowych, a każdy system jest odrębną, oddzielną całością.

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

1. Pomieszczenia w obszarze bezpieczeństwa są zamykane w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.

2. Klucze do pomieszczeń przechowywane są w specjalnej szafce w pomieszczeniu nr 9 budynku Urzędu Gminy Ciechocin.
3. Przebywanie w pomieszczeniach w obszarze bezpieczeństwa osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do dostępu do tych danych i za zgodą ABI lub Wójta Gminy, a w czasie jego nieobecności Sekretarza Gminy.
4. Prace związane z zarządzaniem systemami informatycznymi mogą wykonywać jedynie wyznaczeni administratorzy tych systemów lub upoważnieni przez ABI inni pracownicy w obecności administratora systemu.
5. Każda osoba dopuszczona do pracy przy przetwarzaniu danych osobowych:
   - potwierdza własnoręcznym podpisem znajomość ustawy o ochronie danych osobowych; zarządzenie określające politykę bezpieczeństwa oraz instrukcję określającą sposób postępowania w przypadku naruszenia bezpieczeństwa,
   - posiada własne hasło bezpieczeństwa do systemu obsługującego bazę danych,
   - ma przyznany zakres uprawnień umożliwiających wykonywanie zadania.
6. Do pracy z systemami informatycznymi dopuszczani są jedynie uprawnieni pracownicy posiadający indywidualny identyfikator użytkownika i osobiste hasło. Osoby dopuszczone do przetwarzania danych posiadają zakresy czynności określające ich uprawnienia i odpowiedzialność.
7. Główne hasła do systemów informatycznych zmieniane są najdalej co 60 dni. Aktualne hasła w opieczętowanej kopercie są przechowywane w sejfie. Otwarcia koperty z hasłami może dokonać w sytuacjach wyjątkowych upoważniona przez Wójta Gminy osoba.
8. Zabrania się zapisywania i przechowywania identyfikatorów i haseł w miejscach ogólnie dostępnych.
9. Każdy pracownik przetwarzający dane ponosi odpowiedzialność wynikającą z zakresu jego czynności, w szczególności za zniszczenie, nieprawidłową modyfikację, udostępnienie danych osobom trzecim.
10. Zarejestrowania i wyrejestrowania użytkowników systemów informatycznych służących do przetwarzania danych osobowych dokonują administratorzy tych systemów po akceptacji formalnej administratora bezpieczeństwa informacji.
11. Administrator systemu prowadzi ewidencję nadanych indywidualnych identyfikatorów użytkowników zawierającą nazwę użytkownika, jego identyfikator, datę nadania oraz datę wycofania..
12. Administrator systemu prowadzi dziennik systemu zawierający informacje o pracy systemu i wykonywanych w nim informatycznych istotnych czynnościach administracyjnych.
13. Kierownik komórki organizacyjnej wyznacza pracownika, który wykonuję kopię awaryjne, które przechowywane są w zamkniętej szafie Administratora Bezpieczeństwa informacji.
14. Administrator systemu przeprowadza okresowe kontrole zasobów informatycznych, nie rzadziej niż raz na miesiąc, programami antywirusowymi. W przypadku wykrycia wirusa powiadamia administratora bezpieczeństwa informacji i usuwa wirusa posiadanym programem. Dokonanie kontroli i jej wynik odnotowuje się w dzienniku systemu.
15. Zewnętrzne nośniki danych są przed ich użyciem sprawdzane programem antywirusowym.
16. Wgrywanie jakiegokolwiek oprogramowania do systemów informatycznych, na których przetwarzane są dane osobowe, jest możliwe tylko przez administratora systemu lub za jego wiedzą i po akceptacji formalnej administratora bezpieczeństwa informacji.
17. Zasoby informacyjne oraz nośniki z danymi podlegają szczególnej ochronie przed kradzieżą, modyfikacją zawartości, podglądnięciem i kopiowaniem.
18. Zasoby informacyjne, w szczególności wydruki zawierające dane osobowe oraz nośniki z danymi, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym. O ile jest to niezbędne do bieżącej pracy lub wykonywania zleconego zadania.
19. Dane osobowe przekazywane poza obszar bezpieczeństwa muszą być odbierane za potwierdzeniem przez uprawnione osoby, w sposób zapewniający zachowanie poufności danych.
20. Udostępnianie danych pracownikom upoważnionych instytucji odbywa się na zasadach ustalonych oddzielnym przepisami, w zgodzie z niniejszą instrukcją.
21. Zasoby informacyjne, w szczególności wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć zgodnie z zasadami niszczenia dokumentów III klasy tajności wg normy DIN 32757.
22. Dokumenty złożone przez kandydatów do pracy po zakończeniu akcji rekrutacyjnej są przechowywane w sposób uniemożliwiający dostęp do nich.
23. Systemy informatyczne, np. systemy zarządzania bazami danych, przy pomocy których jest zbudowana baza danych osobowych muszą posiadać certyfikat legalności i być na liście produktów serwisowanych przez producenta oprogramowania.

24. Systemy informatyczne muszą być zabezpieczone przed utratą przetwarzanych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
25. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza wyznaczonym obszarem przetwarzania danych osobowych, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
26. Przeznaczone do naprawy urządzenia lub nośniki danych zawierające dane osobowe pozbawia się przed naprawą danych osobowych albo naprawia się je pod nadzorem administratora systemu lub osoby upoważnionej przez kierownika jednostki.
27. Zawierające dane osobowe urządzenia lub nośniki danych przeznaczone do przekazania odbiorcy nieuprawnionemu do otrzymania danych osobowych przed przekazaniem pozbawia się zapisu tych danych w sposób uniemożliwiający ich odtworzenie.
28. Przeznaczone do likwidacji urządzenia lub nośniki danych zawierające dane osobowe, administrator systemu w obecności administratora bezpieczeństwa informacji pozbawia wcześniej zapisu tych danych w sposób uniemożliwiający ich odtworzenie, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odtworzenie. Fakt dokonania likwidacji potwierdza się protokołem.
29. Stanowiska do pracy w sieciach ponadlokalnych nie mogą mieć bezpośredniego ani pośredniego połączenia z zasobami informatycznymi służącymi do przetwarzania danych osobowych.
30. Użytkowanie sieci komputerowych o zasięgu ponadlokalnym do przesyłania danych osobowych powinno być ograniczone w sposób udokumentowany, z oznaczeniem zakresu uprawnień tylko do wskazanych osób, stanowisk, usług.
31. Dopuszczalnym sposobem użytkowania sieci o zasięgu ponadlokalnym jest:
    - pozyskiwanie informacji niezbędnych do działalności służbowej,
    - udostępnianie informacji niezbędnych do działalności służbowej,
    - przesyłanie informacji środkami telekomunikacji publicznej w sposób uzgodniony z administratorem (właścicielem) danych.

VII. W razie stwierdzenia naruszenia ochrony danych osobowych postępujemy zgodnie z Instrukcją postępowania w sytuacji naruszenia Ochrony Danych Osobowych.

WOUT
mgr inż. Jerzy Cieszyński

Załącznik nr 2
do Zarządzenia Nr 27/08
Wójta Gminy Ciechocin
z dnia 20 czerwca 2008

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY CIECHOCIN

I. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:
a. **Urzędzie** - należy przez to rozumieć Urząd Gminy Ciechocin
b. **Administrator Danych Osobowych** - należy przez to rozumieć Wójta Gminy Ciechocin.
c. **Administratorze Bezpieczeństwa Informacji** - należy przez to rozumieć pracownika urzędu lub inną osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danychosobowych,
d. **Administratorze Systemu Informatycznego** - należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,
e. **użytkownika systemu** - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie lub wolontariusz,
f. **sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
g. **sieci rozległej** - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)
h. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
i. **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów,
j. **wykazie zbiorów danych osobowych** – rozumie się przez to wykaz zarejestrowanych, oraz nie podlegających rejestracji zbiorów danych osobowych,
k. **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
l. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

II. Procedury nadawania i zmiany uprawnień do przetwarzania danych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr
   - 101, poz. 926 z późn. zm.),
   - Polityką bezpieczeństwa przetwarzania danych osobowych systemu informatycznego,
   - niniejszym dokumentem.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na stosownym oświadczeniu.
3. Przetwarzanie danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych.
4. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) administratora informacji.

4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
5. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym. Ustanowione hasło, administrator przekazuje użytkownikowi ustnie.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
9. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
10. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
11. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
12. Odebranie uprawnień pracownikowi następuje na pisemny wniosek Administratora Informacji ,któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
13. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
14. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

III. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Przy wyborze hasła obowiązują następujące zasady:
a. minimalna długość hasła - 6 znaków,
b. zakazuje się stosować:
   - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
   - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi
   - literami, w odwrotnym porządku, dublując każdą literę, itp.),
   - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu,
   - numer rejestracyjny samochodu, jego marka, numer dowodu osobistego,
   - nazwa ulicy na której mieszka lub pracuje, itp.
   - przewidywalnych sekwencji znaków z klawiatury np.: QWERTY","12345678",itp.
c. należy stosować:
   - hasła zawierające kombinacje liter i cyfr,
   - hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole:@, #, &, itp. o ile system informatyczny na to pozwala
   - hasła, które można zapamiętać bez zapisywania,
   - hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,
10. Zmiany hasła nie wolno zlecać innym osobom.

11. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
12.Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
a. Administrator Bezpieczeństwa Informacji
b. Wójt oraz Sekretarz Gminy Ciechocin

IV. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej.
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
6. Przypadki stwierdzenia nieprawidłowości systemu należy zgłaszać do Administratora Systemu.

V. Procedury tworzenia zabezpieczeń

Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji.

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

A. Elektroniczne nośniki informacji
1. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa -zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę urzędu.
2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce Bezpieczeństwa przetwarzania danych osobowych urzędu.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
6. 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.

B. Kopie zapasowe
1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w sejfie urzędu.
2. Dostęp do ww. sejfu mają tylko upoważnieni pracownicy.

C. Wydruki
1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.

3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

VII. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi.

1. Na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika dyskietki.

VIII. W razie stwierdzenia naruszenia ochrony danych osobowych postępujemy zgodnie z Instrukcją postępowania w sytuacji naruszenia Ochrony Danych Osobowych.

IX. Zasady udostępniania danych oraz rejestracji zbiorów danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie na wniosek do Administratora Danych.
2. Udostępnienie zbiorów danych może nastąpić po wyrażeniu zgody przez Administratora Danych oraz Administratora Bezpieczeństwa Informacji. Zgoda nie jest wymagana, jeśli udostępnienie danych wynika z zakresu zadań tej jednostki organizacyjnej Gminy, w dyspozycji której znajdują się te dane,
3. Administrator Bezpieczeństwa Informacji może odmówić udostępnienia danych jeżeli może to naruszyć bezpieczeństwo i ochronę danych zgromadzony w Systemie Informatycznym Urzędu Gminy.
4. Administrator Danych Osobowych i Administrator Bezpieczeństwa Informacji wspólnie opracowują wniosek o rejestrację zbioru danych osobowych.

X. Połączenie do sieci Internet

1. Połączenie lokalnej sieci komputerowej urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych oraz kompleksowego oprogramowania antywirusowego.
2. Do zabezpieczenia sieci należy stosować
a. Firewall,
b. Systemy wykrywania włamań IDS
c. Rejestracja wszelkich zdarzeń w dziennikach systemowych
d. Systemy antywirusowe i antyszpiegowskie.

WÓJT
mgr inż. Jerzy Ciszewski

Załącznik Nr 3
do zarządzenia Nr 27/08
Wójta Gminy Ciechocin
z dnia 20 czerwca 2008

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

I. Postanowienia ogólne

1) Instrukcję opracowano na podstawie:
   - ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.),
   - rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521),
   - wewnętrznego regulaminu ochrony danych osobowych.
2) Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, 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 telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń danych.
3) Osobą odpowiedzialną 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, jest wyznaczony przez administratora danych osobowych – Administrator Bezpieczeństwa Informacji.

II. Tryb i zasady postępowania w przypadku stwierdzenia naruszenie zabezpieczenia systemu informatycznego

1) W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego (włamania do systemu) osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji lub inną upoważnioną przez niego osobę.
2) Administrator Bezpieczeństwa Informacji (lub inna upoważniona osoba) po otrzymaniu powiadomienia:
   - podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł),
   - zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   - ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
   - niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
   - dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
   - sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu (włamaniu do systemu), opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
3) Raport wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych jednostki.
4) Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych Osobowych podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu w przyszłości.

III. Tryb postępowania w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych z uwagi na stan urządzeń, sposób działania programu, jakość komunikacji w sieci telekomunikacyjnej, zawartość zbioru danych osobowych, ujawnione metody pracy

1) Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji lub inną upoważnioną przez niego osobę.
2) Administrator Bezpieczeństwa Informacji (lub inna upoważniona osoba) po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):
   - sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   - sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),
   - sprawdza jakość komunikacji w sieci telekomunikacyjnej,
   - sprawdza zawartość zbioru danych osobowych,
   - poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.
3) W przypadku stwierdzenia naruszenia zabezpieczeń danych:
   - podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, blokuje dostęp do sieci telekomunikacyjnej, do programów oraz zbiorów danych, itp.),
   - zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   - niezwłocznie przywraca prawidłowy stan działania systemu,
   - dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia,
   - sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
4) Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych jednostki.
5) Administrator Bezpieczeństwa Informacji, w porozumieniu z Administratorem Danych Osobowych podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
   - jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
   - jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągniecie konsekwencji prawem przewidzianych.

IV. Postanowienia końcowe

1) Każda osoba wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zobowiązana jest do zapoznania się z niniejszą instrukcją. Wykonanie powyższego zobowiązania pracownik potwierdza własnoręcznym podpisem.
2) Wszelkie zmiany powyższej instrukcji skutkują wobec osób, których dotyczą, z dniem ich doręczenia na piśmie.

WÓJT
mgr inż. Jerzy Cieszyński