WÓJT GMINY
CZŁUCHÓW

Zarządzenie Nr 38/11
Wójta Gminy Człuchów
z dnia 24 czerwca 2011r.
w sprawie polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (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 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. z 2004 r. nr 100 poz. 1024 ze zm.)

zarządza się, co następuje:

§ 1

Wprowadza się :

1. „Politykę bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów", określoną w załączniku nr 1 do niniejszego zarządzenia,
2. „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów", określoną w załączniku nr 2 do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Adam Marciniak

Załącznik nr 1
do Zarządzenia Nr 38/11
Wójta Gminy Człuchów
z dnia 24 czerwca 2011r.

Polityka bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów

1. Wstęp

W systemie Urzędu Gminy Człuchów przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.). Osobą odpowiedzialną za właściwy i niezakłócony przebieg przetwarzania danych w tym systemie jest Administrator Bezpieczeństwa Informacji.

2. Definicje

a) Urząd – w tym dokumencie jest rozumiany, jako Urząd Gminy Człuchów, z siedzibą Człuchowie , ul. Szczecińska 33.
b) Administrator Bezpieczeństwa Informacji (ABI) – pracownik urzędu wyznaczony przez Administratora Danych Osobowych (Wójta) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Urzędzie Gminy Człuchów
c) Użytkownik systemu – 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 lub praktykę w urzędzie.
d) Identyfikator użytkownika – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
e) Sieć lokalna – połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.
f) Sieć publiczna – sieć telekomunikacyjna, nie będąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z poźn. zm.).
g) Sieć telekomunikacyjna – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz.852, z późń. zm.).
h) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
i) Przetwarzanie danych – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
j) Zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
k) Teletransmisja – przesyłanie informacji za pomocą sieci telekomunikacyjnej.
l) Poufność danych – jest to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

m) Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione, lub zniszczone w sposób nieautoryzowany.
n) Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
o) Aplikacja – program komputerowy wykonujący konkretne zadanie.
p) Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.
q) Komórka organizacyjna – rozumie się przez to referat, samodzielne stanowisko pracy.

3. Obowiązki Administratora Bezpieczeństwa Informacji

a) Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
b) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
c) Kontrola nad danymi osobowymi wprowadzanymi do zbiorów, (przez kogo zostały wprowadzone, komu są przekazywane).
d) Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, lub podejrzenia naruszenia zabezpieczeń.
e) Nadzór nad naprawami, konserwacją, oraz likwidacją urządzeń, na których zapisane są dane osobowe.
f) Nadzór nad obiegiem, oraz przechowywaniem dokumentów zawierających dane osobowe.
g) Nadzór nad prawidłowością archiwizacji, oraz usuwania danych osobowych.
h) Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.
i) Nadzór nad prowadzeniem odpowiedniej dokumentacji.

4. Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych w systemie stanowią pomieszczenia budynku Urzędu Gminy Człuchów ul. Szczecińska 33. Kopie zapasowe zawierające zbiory danych osobowych przechowywane są w kasecie stalowej w budynku Urzędu Gminy.

5. Zbiory danych osobowych przetwarzanych w systemie informatycznym Urzędu.

W systemie zbierane są dane zawierające informacje o osobach będących klientami urzędu, które przetwarzane są zgodnie z prawem lub zgodziły się na ich przetwarzanie. W skład systemu wchodzą:

a. Dokumentacja papierowa (korespondencja obywateli, firm, innych instytucji publicznych i niepublicznych, formularze zgody na przetwarzanie danych osobowych itd.)
b. Urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.
c. Wydruki komputerowe.

6. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i wyćwiczalności danych przetwarzanych w systemie:

a) Środki ochrony fizycznej: urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi. Dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym. Zastosowano kasetę stalową do przechowywania nośników z kopiami zapasowymi zawierających dane osobowe.
b) Środki sprzętowe, informatyczne i telekomunikacyjne: stosuje się niszczarki dokumentów. Serwery, na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania. Sieć lokalna podłączona jest do Internetu poprzez router spełniający jednocześnie funkcję sprzętowego,

zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną. Kopie zapasowe wykonywane są codziennie na dysku przenośnym.

c) Środki ochrony w ramach oprogramowania urządzeń teletransmisji: na komputerach użytkowników systemu działa program antywirusowy. Na komputerach użytkowników systemu działa programowy firewall. Dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.
d) Środki ochrony w ramach oprogramowania systemu: dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika. Zastosowano działający w tle program antywirusowy na komputerach użytkowników. W systemie sieciowym stosuje się mechanizm wymuszający okresową zmianę haseł dostępu.
e) Środki ochrony w ramach systemu użytkowego: komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym. Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika. Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika.
f) Środki organizacyjne: wyznaczono Administratora Bezpieczeństwa Informacji. Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.
g) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych (Zał. nr 3) Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych. Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy.

7. Procedura postępowania w przypadku naruszenia ochrony danych osobowych

a. Każdy pracownik urzędu, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to Administratorowi Bezpieczeństwa Informacji.
b. W razie braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, należy zawiadomić bezpośredniego przełożonego
c. Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji należy: niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony (o ile to możliwe), ustalić przyczynę i sprawcę naruszenia ochrony, rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia, o ile to możliwe należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia ochrony i udokumentowanie zdarzenia podjąć stosowne działania, jeśli zaistniały przypadek został przewidziany w dokumentacji systemu operacyjnego, bazy danych, czy instrukcji aplikacji użytkowej, nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji.
d. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych Administrator Bezpieczeństwa Informacji podejmuje następujące kroki: zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy urzędu, może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem, rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora

Danych Osobowych, nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

e. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport według wzoru stanowiącego załącznik Nr 2, który zawiera następujące informacje: wskazanie osoby zawiadamiającej o naruszeniu, oraz innych osób zaangażowanych w wyjaśnienie okoliczności naruszenia bezpieczeństwa, określenie czasu i miejsca zawiadomienia o naruszeniu bezpieczeństwa, jak i samego naruszenia (o ile da się ustalić), określenie okoliczności towarzyszących i rodzaju naruszenia, opis podjętego działania wraz z wyjaśnieniem wyboru sposobu działania, wstępną ocenę przyczyn wystąpienia naruszenia bezpieczeństwa, ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego
f. Raport z wystąpienia zdarzenia Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych.
g. Administrator Bezpieczeństwa Informacji zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych).
h. Zaistniałe naruszenie bezpieczeństwa może stać się przedmiotem zespołowej analizy przeprowadzanej przez kierownictwo urzędu i osób wskazanych przez Administratora Danych Osobowych.
i. Analiza ta powinna zawierać wszechstronną ocenę zaistniałego naruszenia bezpieczeństwa, wskazanie odpowiedzialnych, wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

8. Postanowienia końcowe.

a) Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła
b) odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.
c) Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencje osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru określonego w załączniku Nr 1.

9.Załączniki

1. Załącznik Nr 1. Raport z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów.
2. Załącznik Nr 2. Wykaz osób, które zostały zapoznane z „Polityką Ochrony Danych Osobowych w Urzędzie Gminy Człuchów" oraz „Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów".
3. Załącznik Nr 3 Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Człuchów.

WÓJT
Adam Marciniak

Załącznik nr 1
do Polityki bezpieczeństwa danych osobowych
w Urzędzie Gminy Człuchów

Raport z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów

1. Data:.....Godzina:.....
(dd.mm.rrrr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

1. Lokalizacja zdarzenia:

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

2. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

.....

3. Podjęte działania:

.....

.....

4. Przyczyny wystąpienia zdarzenia:

.....

.....

5. Postępowanie wyjaśniające:

.....

.....

.....
data, podpis Administratora Bezpieczeństwa Informacji

wójt
Adam Marciniak

Załącznik nr 2
do Polityki bezpieczeństwa danych osobowych
w Urzędzie Gminy Człuchów

Wykaz osób,

które zostały zapoznane z „Polityką bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów" oraz „Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów"

Przyjąłem/am/ do wiadomości i stosowania.

Lp	Nazwisko i imię	Komórka organizacyjna	Data, podpis

Adam Marciniak

Załącznik nr 3
do Polityki bezpieczeństwa danych osobowych
w Urzędzie Gminy Człuchów

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Człuchów.

Lp	Nazwisko i imię	Komórka organizacyjna

Adam Marciniak

Załącznik nr 2
do Zarządzenia Nr 38/11
Wójta Gminy Człuchów
z dnia 24 czerwca 2011r.

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów

I. Wprowadzenie

Celem Instrukcji Zarządzania System Informatycznym jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Człuchów, oraz minimalizowanie incydentów mogących zagrozić bezpieczeństwu systemu.
Podstawa prawna tego dokumentu: rozporządzenie 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) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.).

II. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

a. urzędzie – należy przez to rozumieć Urząd Gminy Człuchów,

b. Administratorze Danych Osobowych – należy przez to rozumieć Wójta Gminy Człuchów,

c. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika urzędu wyznaczonego do nadzorowania i przestrzegania zasad ochrony, określonych w niniejszym dokumencie, Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Człuchów, oraz wymagań w zakresie ochrony wynikających z powszechnie wynikających przepisów o ochronie danych osobowych, odpowiedzialny za funkcjonowanie systemu, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie.

d. użytkownika systemu - 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 w urzędzie,

e. sieci lokalnej - połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,

f. sieci rozległej (publicznej) - sieć telekomunikacyjna, nie będąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z pożń. zm.),

g. danych osobowych - rozumie się przez to wszystkie informacje dotyczące zidentyfikowanej lub możliwej od zidentyfikowania osoby fizycznej, i. zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych wg określonych

kryteriów, j. wykazie zbiorów danych osobowych – rozumie się przez to wykaz zarejestrowanych jak i nie podlegających rejestracji zbiorów danych osobowych,

h. przetwarzaniu danych - rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,

i. systemie informatycznym - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

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

1) Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
2) polityką bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów
3) niniejszym dokumentem

4) Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na wykazie, którego wzór stanowi Załącznik nr 2 do „Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów"

5) Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego służącego do przetwarzania danych osobowych na podstawie pisemnego upoważnienia Administratora Danych Osobowych określającego zakres uprawnień pracownika, którego wzór stanowi załącznik nr 4 do „Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Człuchów".

6) Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła, oraz ustanowienia zakresu dostępnych danych i operacji.

7) Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji jest przekazywane użytkownikowi ustnie. Hasło to należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.

8) Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła.

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 uwierzytelnienie dwustopniowe: na poziomie dostępu do sieci lokalnej, oraz dostępu do aplikacji.

11) 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.

12) 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.

13) Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia, ochrony rejestru użytkowników, oraz ich uprawnień w systemie informatycznym.

14) Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień, oraz umożliwiającego przeglądanie historii zmian uprawnień użytkowników.

IV. Zasady ustalania i posługiwania się hasłami.

a. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
b. Hasło użytkownika musi być zmienione przynajmniej raz w miesiącu.
c. Identyfikator użytkownika nie powinien być zmieniany bez wyraźniej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
d. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
e. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
f. Pracownik nie ma prawa udostępniania swojego hasła innym osobom.
g. Hasło należy wprowadzać w sposób, który uniemożliwi innym osobom jego poznanie.
h. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
i. Przy wyborze hasła występują następujące zasady minimalna długość hasła to 6 znaków, zakazuje się stosować haseł, z których użytkownik korzystał w poprzednim miesiącu, swojej nazwy użytkownika w jakiejkolwiek formie, swojego nazwiska czy imienia w jakiejkolwiek formie, ogólnie dostępnych informacji o użytkowniku takich jak numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka itp. , przewidywalnych sekwencji znaków z klawiatury np. „QWERTY","12345" itp. należy stosować: hasła zawierające kombinacje liter, cyfr i znaków specjalnych, hasła które można zapamiętać bez zapisywania.
j. Zmiany hasła nie można zlecać innym osobom.

V. Procedury rozpoczęcia, zawieszania i zakończenia pracy w systemie.

a. Przed rozpoczęciem pracy z komputerem należy zalogować się do systemu informatycznego przy użyciu własnego indywidualnego identyfikatora i hasła.
b. W sytuacji opuszczenia stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu.
c. Przed wyłączeniem komputera należy zakończyć pracę wszystkich używanych programów i wykonać o ile to możliwe prawidłowe zamknięcie systemu.

d. Niedopuszczalne jest wyłączanie komputera bez prawidłowego zamknięcia wszystkich programów i wylogowania z sieci komputerowej.
e. Przypadki nieprawidłowej pracy systemu informatycznego należy niezwłocznie zgłaszać do Administratora Bezpieczeństwa Informacji

VI. Kopie bezpieczeństwa danych osobowych.

a. Kopie bezpieczeństwa danych osobowych przygotowywane są przez Administratora Bezpieczeństwa Informacji
b. Kopie wykonywane są codziennie na dydku przenośnym.
c. Dysk przenośny po archiwizacji przechowywany jest w kasecie stalowej w zamkniętym pomieszczeniu.

VII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

1. Elektroniczne nośniki informacji.
   a. Dane osobowe w postaci elektronicznej (nie licząc kopii bezpieczeństwa) zapisane na dyskietkach, dyskach magnetooptycznych, 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 Człuchów).
   c. Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane wyłącznie w zamykanych szafach.
   d. 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.
   e. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych. W przypadku, gdy nie 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. Ochrona przed złośliwym oprogramowaniem.

1. Każdy komputer służący do przetwarzania danych osobowych jest wyposażony w działający cały czas program antywirusowy. Program antywirusowy aktualizowany jest automatycznie przynajmniej raz na dwie godziny.

2. Cały ruch sieciowy z siecią publiczną monitorowany jest na bieżąco przez bramę antywirusową w routerze sieciowym.
3. Zabrania się stosowania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Za skanowanie odpowiedzialny jest użytkownik komputera.
4. Poczta elektroniczna jest automatycznie sprawdzana przez skaner antywirusowy.
5. Wykrycie wirusa użytkownik komputera ma obowiązek zgłosić natychmiast Administratorowi Bezpieczeństwa Informacji

IX. Połączenie do sieci Internet.

1. Połączenie z siecią Internet (siecią publiczną) zabezpieczone jest przez moduł firewall działający na routerze sieciowym.
2. Na każdym komputerze w systemie informatycznym urzędu działa osobny firewall.
3. Zabronione jest połączenie z siecią Internet z niedziałającym programem antywirusowym (lub jego brakiem) i firewallem.

WÓJT
Adam Marciniuk