WÓJT GMINY POCZESNA
ul. Wolności 2
42-262 Poczesna

Załącznik nr 2 do
Zarządzenia nr 0151/169/09
Wójta Gminy Poczesna
z dnia 12 marca 2009r.

POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY POCZESNA

Rozdział I
Wprowadzenie

1. Wprowadzenie Polityki Bezpieczeństwa jest wymogiem ustawowym i jest regulowana następującymi aktami prawnymi:
   a) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2001 r. Nr 101, poz. 926 z późn. zm.)
   b) rozporządzenie 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),
   c) rozporządzenie Prezesa Rady ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. z 1999 r. Nr 18 poz. 162)

2. Polityka bezpieczeństwa ochrony danych osobowych jest zestawem reguł i praw regulujących sposób zarządzania, przetwarzania, przechowywania i dystrybucji danych osobowych ze zbiorów pozostających w Urzędzie Gminy w Poczesnej.
3. Celem polityki bezpieczeństwa jest zapewnienie maksymalnego poziomu bezpieczeństwa procesu przetwarzania danych osobowych i ochrony przed nieuprawnionym dostępem i ich modyfikacją, utratą poufności przy zachowaniu integralności i rozliczalności danych, poprzez właściwą organizację oraz wprowadzenie i realizację odpowiednich działań przy wykorzystaniu środków technicznych.

4. Niniejsza Polityka bezpieczeństwa zawiera w szczególności:
    a) wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
    b) wykaz zbiorów danych osobowych,
    c) środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
5. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
    a) stwierdzono naruszenie zabezpieczeń systemu informatycznego,
    b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

6. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Gminy Poczesna.
7. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w Urzędzie Gminy Poczesna.

8. Administratorem Danych jest Wójt Gminy Poczesna.
Przez **administratora danych** rozumie się organ, jednostkę organizacyjną, podmiot lub osobę, wobec których ustawa znajduje swoje zastosowanie zgodnie z dyspozycja art. 3 ustawy, a które decydują o celach i środkach przetwarzania danych. Administratorem danych są więc wszystkie podmioty realizujące zadania publiczne jeżeli przetwarzają dane osobowe. Szczególne kompetencje administratora danych, jako decydującego o środkach i celach przetwarzania danych, konkretyzują się w formie nałożonych na niego obowiązków i przyznanych uprawnieniach.

9. Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, [aneks do załącznik nr]
10. Administrator Bezpieczeństwa Informacji realizuje zadania z zakresu ochrony danych, a w szczególności:

    a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,

b) podejmowanie stosownych działań zgodnie z niniejszą Polityką Bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

c) niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej w przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

d) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

Rozdział II

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Środki ochrony fizycznej

    a) Budynek Urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest nadzorowany przez straż miejską całą dobę (zamykany po zakończeniu pracy).

    b) Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami.

    c) W pomieszczeniu serwera zainstalowano żaluzje antywłamaniowe, oraz klimatyzację.

    d) Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności kierownika działu.

    e) Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

    f) W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

    g) Do przebywania w pomieszczeniu serwera uprawnieni są: administrator bezpieczeństwa informacji, osoby odpowiedzialne za obsługę informatyczną Urzędu oraz kierownik urzędu.

    h) Przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 8, a w przypadku ich nieobecności - w obecności osoby pisemnie upoważnionej przez kierownika urzędu.

2. Środki sprzętowe, informatyczne i telekomunikacyjne

    a) Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki dokumentów)

    b) Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej, komputer spełniający role Serwera oraz sieć lokalna podłączona do Internetu za pomocą Router'a. Zastosowano oprogramowanie do tworzenia kopii zapasowych.

c) Na wszystkich stacjach roboczych oraz serwerze zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do użytkownika.

d) Kopie awaryjne wykonywane są na nośnikach taśmowych i płytach CD-R

3. Środki ochrony w ramach oprogramowania systemu

a) Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługą informatyczną Urzędu

b) Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji

c) System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu

d) W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

a) Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji

b) Dla każdego użytkownika systemu jest ustalony odrębny identyfikator

c) Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło)

5. Środki ochrony w ramach systemu użytkowego

a) Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika

b) Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym

c) Zabrania się instalować jakiegokolwiek oprogramowania przez użytkownika

6. Środki organizacyjne

a) Wyznaczono administratora bezpieczeństwa informacji, który przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia kierownika urzędu określającego zakres uprawnień pracownika.

b) Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do pracy z tymi danymi szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.

c) Prowadzona jest ewidencja osób upoważnionych do przetwarzaniu danych osobowych

d) Wprowadzono instrukcję zarządzania systemem informatycznym

e) Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych

f) Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.

g) Określono sposób postępowania z nośnikami informacji.

Rozdział 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.
        - wyrazów słownikowych,

- 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) Kierownik Urzędu lub osoba przez niego wyznaczona

Rozdział 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 zablokowania lub wymeldowania z systemu, 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 (polecenie: logout).
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

Rozdział V

Opis zdarzeń naruszających ochronę danych osobowych

Zdarzeniami naruszającymi ochronę danych osobowych bądź stwarzającymi podejrzenie naruszenia zabezpieczeń tych danych mogą być następujące przypadki:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana itp.

b) niewłaściwe parametry środowiska, takie jak np. nadmierna wilgotność, byt wysoka temperatura, oddziaływanie pola elektromagnetycznego,

c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na celowe działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,

d) komunikaty alarmujące o próbie naruszenia zabezpieczeń systemu, który zapewnia ochronę danych bądź komunikat o podobnym znaczeniu,

e) odstępstwa od prawidłowego stanu danych wskazujące na niewłaściwe działanie systemu i niepożądaną jego modyfikację,

f) naruszenie lub próba naruszenia integralności systemu bazy danych w tym systemie,

g) modyfikacja lub próba modyfikacji danych oraz zmiana w strukturze danych dokonana bez odpowiedniego upoważnienia (autoryzacji),

h) stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie,

i) ujawnienie danych osobowych lub objętych tajemnicą procedur ochrony danych osobowych osobom nieupoważnionym, bądź innych elementów systemu zabezpieczeń,

j) funkcjonowanie sieci komputerowej lub praca systemu wykazuje nieprzypadkowe odstępstwo od prawidłowego rytmu pracy wskazujące na zaniechanie lub przełamanie ochrony danych osobowych - np. praca w sieci lub przy komputerze osoby do tego nieupoważnionej, sygnał o nieautoryzowanym logowaniu, itp., k) ujawnienie istnienia nieautoryzowanych kont dostępu do danych objętych

ochroną

l) zniszczenie lub podmiana nośnika z danymi osobowymi bądź skasowanie lub skopiowanie danych osobowych w sposób niedozwolony lub przez osobę nieupoważnioną,

m) rażące naruszenie dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji np. nie wylogowanie się z systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie wykonanie w określonym terminie kopii bezpieczeństwa, praca na danych osobowych w celach prywatnych, itp.),

n) stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział VI
Zabezpieczenie danych osobowych

1. Obszar, w którym przetwarzane są dane osobowe stanowi budynek Urzędu Gminy Poczesna w miejscowości Poczesna, ul. Wolności 2.
2. Wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi aneks do załącznik
   do Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Gminy Poczesna.
3. Wykaz zbiorów danych osobowych ze wskazaniem formy przetwarzania tych danych stanowi załącznik do Polityki Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Gminy Poczesna.
4. Budynek Urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest zamykany przez sprzątaczki po zakończeniu pracy. W wejściu do budynku zamontowane są drzwi antywłamaniowe zamykane na dwa zamki patentowe, wyjście awaryjne, wejście do piwnicy, okna na parterze i podpiwniczeniu budynku zabezpieczone są kratą stalową. Cały budynek zabezpieczony jest systemem antywłamaniowym uruchamianym po zamknięciu budynku.
5. Urządzenia służące do przetwarzania danych osobowych znajdują się

w pomieszczeniach zabezpieczonych zamkami.

6. Zbiory danych przetwarzane w postaci tradycyjnej są przechowywane w szafach zamykanych na klucz.
7. Przebywanie osób trzecich w pomieszczeniach, gdzie są przetwarzane dane osobowe dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych lub w obecności przełożonego.
8. Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
9. W przypadku przebywania osób postronnych w pomieszczeniach o których mowa wyżej, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
10. Ochronę serwera przed awariami zasilania oraz zakłóceniami sieci energetycznej zapewniają zasilacze UPS - em.
11. Sieć lokalna podłączona jest do sieci publicznej za pomocą urządzenia spełniającego funkcję Router'a.
12. Na poziomie aplikacji służącej do przetwarzania danych osobowych zastosowano identyfikator i hasło dostępu dla upoważnionego pracownika.
13. Stacje robocze, z których możliwy jest dostęp do danych zabezpieczony jest hasłem.
14. Kopie zapasowe wykonywane są na dyskietkach, płytach CD i DVD.

Rozdział VII

Gromadzenie, przepływ oraz opis struktury zbiorów danych osobowych

1. Dane osobowe pozyskiwane są z danych źródłowych i innych zasobów. Dane te gromadzone są w systemach informatycznych, zbiorach manualnych oraz zewnętrznych nośnikach danych.
2. Rozwiązania techniczne stosowane w Urzędzie pozwalają na uzupełnienie tych samych danych z innych posiadanych zasobów w ramach jednostki, co służy efektywniejszemu ich wykorzystaniu w załatwianiu spraw.
3. Przepływ danych następuje w sposób manualny przy wykorzystaniu zewnętrznych

nośników danych oraz za pomocą Elektronicznego Obiegu Dokumentów.

4. Korespondencja z adresatami jest realizowana za pośrednictwem poczty oraz za pomocą Skrzynki Podawczej Urzędu Gminy Poczesna.
5. Gromadzone dane osobowe są udostępniane pracownikom w zakresie niezbędnym do ich pracy.
6. Opis struktury zbiorów danych oraz sposób przepływu danych znajduje się w dokumentacji technicznej eksploatowanych systemów przechowywanej na stanowiskach roboczych.
7. Zakres gromadzonych danych osobowych jest zgodny z przepisami prawa.

Rozdział VIII

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych każda osoba zatrudniona przy przetwarzaniu tych danych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.
2. W przypadku niemożności zawiadomienia Administratora Bezpieczeństwa Informacji, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub upoważnionej osoby, należy:

   a) niezwłocznie podjąć czynności niezbędnego powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia
   c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudniać udokumentowanie i analizę,
   d) podjąć inne stosowne działania przewidziane w instrukcjach technicznych i technologicznych, dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej właściwe dla objawów i sytuacji towarzyszącej naruszeniu,
   e) udokumentować wstępnie zaistniałe zdarzenie,
   f) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia

Administratora Bezpieczeństwa Informacji lub upoważnionej osoby.

4. Po przybyciu na miejsce Administrator Bezpieczeństwa Informacji lub osoba upoważniona:
   a) zapoznaje się z zaistniałą sytuacją, identyfikuje rodzaj zaistniałego zdarzenia i dokonuje wyboru metody dalszego postępowania celem powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych osobowych,
   b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również innych osób mogących posiadać informacje związane z zaistniałym zdarzeniem,
   c) rozważa celowość i potrzebę poinformowania o zaistniałym zdarzeniu Administratora Danych,
   d) w przypadku potrzeby nawiązuje bezpośredni kontakt ze specjalistami spoza Urzędu.
5. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia i powiadomienia,
   c) określenie okoliczności towarzyszących i rodzaju naruszenia,
   d) wybór metody postępowania wraz z opisem podjętych działań i przesłanek skłaniających do ich podjęcia,
   e) wstępną ocenę przyczyn wystąpienia naruszenia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
6. Raport, o którym mowa w pkt. 5, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
8. Zaistniałe zdarzenie powinno stać się przedmiotem szczegółowej analizy przeprowadzonej przez Administratora Danych, Administrator Bezpieczeństwa

Informacji i Pełnomocnika ds. Ochrony Informacji Niejawnych.

9. Analiza powinna zawierać ocenę zaistniałego zdarzenia, wskazanie osób odpowiedzialnych oraz wnioski nt. ewentualnych przedsięwzięć proceduralnych, organizacyjnych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział IX

Postanowienia końcowe

1. Urząd Gminy w Poczesna przetwarza dane osobowe na podstawie przepisów prawa.
2. Dane osobowe mogą być udostępniane zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2001 r. Nr 101, poz. 926 z późn. zm.).
3. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się i stosowania zapisów niniejszego dokumentu oraz przepisów ustawy o ochronie danych osobowych.

Wyk [Adam Szołtys]

Poczesna, dnia r. 02.02.2009r.

WYZNACZENIE
ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

1. *Na podstawie § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 03.06.1998r. 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/ z dniem 02.02.2009 r. wyznacza się*

Pana

Adama Szołtys** zam. **Al. Wojska Polskiego 115, 42-200 Częstochowa

*legitymującego się dowodem osobistym nr **ALY325146***

na ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI.

2. Administrator bezpieczeństwa informacji jest odpowiedzialny 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 zabezpieczeń.

3. Jednocześnie tracą uprawnienia administratora bezpieczeństwa informacji osoby wcześniej wyznaczone do pełnienia tych obowiązków.

podpis
administratora bezpieczeństwa informacji

WÓJT
mgr inż. Krzysztof Ujma

podpis
kierownika urzędu

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW STOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Nazwa pomieszczenia	Rodzaj danych i stosowany program komputerowy.
Nieruchomości Komunalne, Rolnictwo i Leśnictwo p.12	Mienie komunalne, podziały gruntów. Rejestr zezwoleń na utrzymanie psów ras uznanych za agresywne
Księgowość podatkowa Dodatki mieszkaniowe p.4	Rejestr podatków i opłat lokalnych Podatki od osób fizycznych Ewidencja czynszów mieszkaniowych
Planowanie Przestrzenne, Inwestycje, p.14,32 Ochrona Środowiska p. 11	Ewidencja wydanych decyzji o warunkach zabudowy i pozwoleń na budowę. Korespondencja, Przetargi dane uczestników konkursów. Plan urządzania lasów nie stanowiące własność Skarbu Państwa., Ewidencja decyzji na wycięcie drzew
GOPS p.1,2 i 3	Ewidencja podopiecznych GOPS
Księgowość budżetowa,kasa p.9,10,32	Płace.
Biuro Rady Gminy p.30	Akta osobowe radnych
Serwerownia p.16	Programy księgowe i podatkowe
Sekretarz Gminy p.4 Dowody osobiste p. 34	Akta osobowe pracowników, kierowników jednostek organizacyjnych, wójta, zastępcy wójta, Rejestr wydanych dokumentów tożsamości
Sekretariat p.28	Poczta, Skargi i Wnioski
Urząd Stanu Cywilnego	Ewidencja ludności, Księgi stanu cywilnego, Rejestr osób formacji OC i świadczeń rzeczowych na rzecz OC
Działalność Gospodarcza	Rejestry Ewidencji działalności gospodarczej Rejestr pozwoleń na sprzedaż napoi alkoholowych
Fundusz alimentacyjny	Rejestr osób korzystających ze świadczeń alimentacyjnych Komisja Rozwiązywania Problemów Alkoholowych

Nazwa pomieszczenia	Rodzaj danych i stosowany program komputerowy.
Nieruchomości Komunalne, Rolnictwo i Leśnictwo p.7	Ewidencja czynszów mieszkaniowych (Papier) Mienie komunalne (Papier), Podział gruntów (HTML - Internet Explorer) Plan urządzania lasów nie stanowiące własność Skarbu Państwa (Papier)
Księgowość podatkowa p.8	Rejestr zezwoleń na utrzymanie psów ras uznanych za agresywne (Papier) Ewidencja decyzji na wycięcie drzew (Papier) Podatki od osób fizycznych, płace. (Księgowość Podatkowa)
Planowanie Przestrzenne, Inwestycje, Ochrona Środowiska p.9	Ewidencja wydanych decyzji o warunkach zabudowy i pozwoleń na budowę. (Papier) Korespondencja, Przetargi (WORD, Papier) Dane uczestników konkursów. (WORD)
GOPS p.1,2 i 4	Ewidencja podopiecznych GOPS (Świadczenia Rodzinne)
Księgowość budżetowa p.13	Rejestr podatków i opłat lokalnych (Burmistrz)
Biuro Rady Gminy p.14	Akta osobowe pracowników, kierowników jednostek organizacyjnych, wójta, zastępcy wójta, radnych (Papier)
Serwerownia p.16	Programy księgowe i podatkowe
Sekretarz Gminy p.4	Skargi i wnioski (Papier)
Sekretariat p.1	Poczta, Skargi i Wnioski (WORD, Papier)
Urząd Stanu Cywilnego	Ewidencja ludności (ARAM), Dowody osobiste (System Obsługi Dowodów Osobistych) Księgi stanu cywilnego (Papier) Rejestr osób formacji OC i świadczeń rzeczowych na rzecz OC (Papier)
Działalność Gospodarcza	Rejestry Ewidencji działalności gospodarczej (Ewidencja Działalności Gospodarczej) Rejestr pozwoleń na sprzedaż napoi alkoholowych (Papier) Komisja Rozwiązywania Problemów Alkoholowych (Papier)
Biblioteka	Rejestr czytelników Gminnej Biblioteki Publicznej. (Papier)

WYKAZ BUDYNKU I POMIESZCZEŃ TWORZĄCYCH OBSZAR W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

Budynek:

Urzędu Gminy Poczesna

ul.. Wolności 2

42-262 Poczesna

Pomieszczenia:

Nazwa pomieszczenia	Nr pokoju
Nieruchomości Komunalne, Rolnictwo i Leśnictwo	**12**
Księgowość podatkowa	**3**
Planowanie Przestrzenne, Inwestycje, Ochrona Środowiska	**11**
Urząd Stanu Cywilnego	
Księgowość budżetowa, kasa	**9,10,32**
Dowody osobiste	**34**
Biuro Rady Gminy	**30**
Serwerownia	
Sekretarz Gminy	**29**
Sekretariat	**28**
GOPS	**2.3.4**
Działalność Gospodarcza	**34**
Fundusz alimentacyjny	**32**

WYKAZ POMIESZCZEŃ TWORZĄCYCH OBSZAR W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

Nazwa pomieszczenia	Rodzaj danych
Nieruchomości Komunalne, Rolnictwo i Leśnictwo p.12	Mienie komunalne, podziały gruntów. Rejestr zezwoleń na utrzymanie psów ras uznanych za agresywne
Księgowość podatkowa Dodatki mieszkaniowe p.4	Rejestr podatków i opłat lokalnych Podatki od osób fizycznych Ewidencja czynszów mieszkaniowych
Planowanie Przestrzenne, Inwestycje, p.14,32 Ochrona Środowiska p. 11	Ewidencja wydanych decyzji o warunkach zabudowy i pozwoleń na budowę. Korespondencja, Przetargi dane uczestników konkursów. Plan urządzania lasów nie stanowiące własność Skarbu Państwa., Ewidencja decyzji na wycięcie drzew
GOPS p.1,2 i 3	Ewidencja podopiecznych GOPS
Księgowość budżetowa,kasa p.9,10,32	Płace.
Biuro Rady Gminy p.30	Akta osobowe radnych
Serwerownia p.16	Programy księgowe i podatkowe
Sekretarz Gminy p.4 Dowody osobiste p. 34	Akta osobowe pracowników, kierowników jednostek organizacyjnych, wójta, zastępcy wójta, Rejestr wydanych dokumentów tożsamości
Sekretariat p.28	Poczta, Skargi i Wnioski
Urząd Stanu Cywilnego	Ewidencja ludności, Księgi stanu cywilnego, Rejestr osób formacji OC i świadczeń rzeczowych na rzecz OC
Działalność Gospodarcza	Rejestry Ewidencji działalności gospodarczej Rejestr pozwoleń na sprzedaż napoi alkoholowych
Fundusz alimentacyjny	Rejestr osób korzystających ze świadczeń alimentacyjnych Komisja Rozwiązywania Problemów Alkoholowych