Zarządzenie Nr 5/2012
Wójta Gminy Czarnia
z dnia 01 marca 2012 r.

w sprawie wdrożenia do stosowania w Urzędzie Gminy Czarnia „Polityki bezpieczeństwa Urzędu Gminy Czarnia" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarnia".

Na podstawie art. 26 i 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r., Nr 101, póz. 926 ze zm.) i § 3, 4, 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, póz. 1024).

zarządzam, co następuje:

§1.

Wprowadzić „Politykę bezpieczeństwa Urzędu Gminy Czarnia" i „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarnia" do przestrzegania i stosowania przez pracowników Urzędu Gminy Czarnia zgodnie z załącznikami nr l i 2 do zarządzenia.

§2.

Zobowiązuję wszystkich pracowników Urzędu do zapoznania się w terminie do 15 marca 2012 roku z treścią „Polityki bezpieczeństwa Urzędu Gminy Czarnia" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarnia" potwierdzonego podpisem w stosownym wykazie oraz do przyjęcia i podpisania upoważnień zezwalających na przetwarzanie danych osobowych.

§3.

Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§4.

Zarządzenie wchodzi w życie z dniem podpisania.

W Ó J T
inż. Czesław Jurga

Załącznik nr 1 do
Zarządzenia Nr 5/2012
Wójta Gmin Czarnia
z dnia 01 marca2012 r.

Polityka bezpieczeństwa
Urzędu Gminy Czarnia

Podstawa prawna

§1.

Paragraf 3 i 4 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, póz. 1024).

Postanowienia ogólne

§2.

1. Ilekroć mowa w niniejszym dokumencie o Polityce, należy przez to rozumieć „Politykę bezpieczeństwa Urzędu Gminy Czarnia".
2. Ilekroć mowa w niniejszym dokumencie o Urzędzie należy przez to rozumieć Urząd Gminy Czarnia.
3. Ilekroć mowa w niniejszym dokumencie o Wójcie należy przez to rozumieć Wójta Gminy Czarnia.

§3.

Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu jest Wójt.

§4.

Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu. W celu zrealizowania tych obowiązków administrator danych wprowadza Politykę bezpieczeństwa jako dokument obowiązujący w Urzędzie.

Zagadnienia organizacyjne

1. Kierownictwo Urzędu wyznacza Administratora bezpieczeństwa informacji, Administratora systemu informatycznego oraz osobę upoważnioną do

zastępowania Administratora bezpieczeństwa informacji.

W związku z faktem, iż w części zadania Administratora bezpieczeństwa informacji i Administratora systemu informatycznego pokrywają się dopuszcza się możliwość wyznaczenia na te stanowiska jednej osoby.

2. Do Kierownictwa Urzędu należy zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do przetwarzania i przechowywania danych osobowych, zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych.
3. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się i przestrzegania Polityki.
4. Osoba przetwarzająca dane osobowe składa oświadczenie o zapoznaniu się z przepisami i odpowiedzialności karnej za naruszenie ochrony danych osobowych oraz zachowaniu tajemnicy, którego wzór stanowi **załącznik. nr l do Polityki.**
5. Fakt zapoznania się z Polityką pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi **załącznik nr 2 do Polityki.**
6. Pracownikom wolno przebywać na terenie Urzędu tylko w godzinach ich pracy, a po godzinach pracy - po zawiadomieniu bezpośrednio przełożonego.

   Przebywanie na terenie Urzędu w dni wolne od pracy wymaga zezwolenia Wójta.
7. Korzystanie z systemu informatycznego służącego do przetwarzania danych osobowych może odbywać się tylko w godzinach pracy Urzędu, a po godzinach pracy - po zawiadomieniu bezpośrednio przełożonego.

Wykaz zbiorów danych osobowych i pomieszczeń, w których są przetwarzane

§6.

Wszystkie zbiory wymienione w poniższej tabeli znajdują się w budynku Urzędu Gminy Czarnia, Czarnia 41, 07-431 Czarni

L/p	*Zbiór danych*	*Nazwa oprogramowania (producent)*	*Nr pokoju*
1.	**Ewidencja ludności i rejestr wyborców**	**System Ewidencji Ludności - SELWIN wraz z modułem Rejestr Wyborców RWWIN (SIGNITY S.A)**	**5**
2.	**Baza osób składających wnioski w sprawie wydawania dowodów osobistych**	**System Wydawania Dowodów Osobistych (WASKO S.A)**	**5**
3.	**Rejestr płatników podatku od nieruchomości , leśnego , rolnego**	**PODATKI (Usługi Informatyczne INFO - SYSTEM)**	**6**
4.	**Rejestr płatników podatku od nieruchomości , leśnego , rolnego**	**Księgowość zobowiązań (Usługi Informatyczne INFO – SYSTEM)**	**6**

5.	Baza płatników składek podatku od środków transportowych	AUTA (Usługi Informatyczne INFO – SYSTEM)	6
6.	Rejestr osób (pracowników) do celów kadrowych	POLSKI SYSTEM KADROWO – PŁACOWY (POLSKIE CENTRUM KADROWO – PŁACOWE)	13
7.	Baza płatników składek ZUS (pracowników)	PŁATNIK (PROKOM Software S.A)	13

Sposób przepływu danych

§7.

1. W budynku Urzędu brak jest wewnętrznej sieci informatycznej. Bazy danych zawierające dane osobowe umiejscowione są na stacjach roboczych.
2. Możliwe przepływy danych między oprogramowaniem przetwarzającym bazy danych zawierające dane osobowe:

    1) Podatki < - > Księgowość zobowiązań
    2) Polski System Kadrowo-Płacowy - > Płatnik

§8.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi załącznik **nr 3 do Polityki .**

Zabezpieczenia fizyczne

§8.

1. Wejście do budynku Urzędu zabezpieczone winno być przynajmniej zamkami drzwiowymi.

    Do budynku Urzędu dostać można się wejściem głównym:

2. Poszczególne pokoje, w których odbywa się przetwarzanie danych i ich składowanie muszą być wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności pracownika. Po zakończeniu pracy osoba zamykająca pomieszczenie powinna przekazać klucz sprzątaczce, bądź umieścić go w specjalnie przeznaczonej gablotce.
3. Stanowiska komputerowe w pomieszczeniach gdzie mogą przebywać osoby nieupoważnione do przetwarzania danych osobowych (np. interesanci albo inni pracownicy Urzędu) winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych. W pokoju, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie.

4. W przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu lub blokowanie systemu, których dezaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.
5. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
6. Kopie bezpieczeństwa (kopie zapasowe) wykonują okresowo pracownicy w ramach swoich obowiązków. Kopie bezpieczeństwa przechowywane są w szafie metalowej pok. nr 10 Urzędu. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
7. Wydruk z ważnym hasłem należy przechowywać tak by uniemożliwić dostęp do niego osobom postronnym (innym niż sam użytkownik, przełożeni i Administratorzy).

Zabezpieczenia nie fizyczne

§9.

1. Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji. Nieudane próby logowania są rejestrowane, a po 3 nieudanych próbach logowania następuje czasowa blokada konta użytkownika na stacji roboczej.
2. Dostęp do systemu stacji roboczych chroniony jest hasłem.
3. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny (dodatkowy, oprócz systemowego) system autoryzacji użytkownika.
4. Wykorzystany jest system szyfrowania danych (dostępny w systemie operacyjnym) uniemożliwiający odczyt danych osobom nieupoważnionym.
5. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się programową zaporę ogniową (ang. firewall) .
6. Zgodnie z przyjętym harmonogramem wykonuje się kopie bezpieczeństwa.

Monitorowanie zabezpieczeń

§10.

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:
   1) Administrator danych
   2) Administrator bezpieczeństwa informacji
   3) Administrator systemu informatycznego
2. W ramach monitoringu należy przeprowadzać następujące działania:
   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
   2) sprawdzania częstotliwości zmian haseł.
3. Administrator bezpieczeństwa informacji sporządza roczne plany kontroli zatwierdzone przez Administratora danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
4. Na podstawie zgromadzonych materiałów, o których mowa w ust. 3. Administrator bezpieczeństwa informacji sporządza roczne sprawozdanie i przedstawia Administratorowi danych.

Obowiązki Administratora danych

§11.

1. Do obowiązków Administratora danych należy w szczególności:
   1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobieganie zabraniu danych przez osobę nieuprawnioną,
   3) zapobieganie przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych,
   4) zbieranie danych dla oznaczonych, zgodnych z prawem celów,
   5) dbałość o merytoryczną poprawność danych i adekwatność w stosunku do celów w jakich są przetwarzane.
   6) opracowanie instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych,

7) określanie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

8) opracowanie instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,

9) prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych,

10) organizowanie szkoleń mających na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

2. Administrator danych odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:

1) ochronę danych przed niepowołanym dostępem,

2) nieuzasadnioną modyfikację lub zniszczenie danych,

3) nielegalne ujawnienie danych.

w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

3. Zgłasza zbiory danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Obowiązki Administratora bezpieczeństwa informacji

§12.

Do obowiązków Administratora bezpieczeństwa informacji należy w szczególności:

1) nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym,

2) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane dane osobowe,

3) podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych,

4) badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,

5) podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych,

6) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe,

7) przeprowadzanie symulowanych włamań do systemu w celu ustalenia aktualnego poziomu zabezpieczeń,

8) nadzór nad wykonywaniem kopii zapasowych i przechowywaniem,

9) wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych,

10) sporządzanie planów kontroli zatwierdzanych przez Administratora danych

przeprowadzanie zgodnie z nimi kontroli,

11) sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Obowiązki Administratora systemu informatycznego

§13.

Do obowiązków Administratora systemu informatycznego należy w szczególności:

1) naprawa, konserwacja oraz likwidacja urządzeń komputerowych zawierających dane osobowe,
2) definiowanie użytkowników i haseł dostępu w systemie,
3) aktualizowanie oprogramowania systemowego, chyba że aktualizacje wykonywane są automatycznie,
4) aktualizowanie oprogramowania antywirusowego, chyba że aktualizacje wykonywane są automatycznie,
5) okresowe sprawdzanie kopii zapasowych pod kątem ich dalszej przydatności.

Postępowanie w przypadku naruszenia ochrony danych osobowych

§14.

1. Każdy pracownik Urzędu, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informację o mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi bezpieczeństwa informacji.
2. W razie niemożliwości zawiadomienia Administratora bezpieczeństwa lub osoby upoważnionej do zastępowania Administratora bezpieczeństwa, należy powiadomić bezpośredniego przełożonego.
3. W przypadku wykrycia naruszenia ochrony danych osobowych Administrator bezpieczeństwa informacji lub osoba upoważniona do jego zastępowania informuje kierownictwo Urzędu o zaistniałym zdarzeniu oraz przeprowadza wstępne dochodzenie, po czym sporządza raport opisujący okoliczności zdarzenia, którego wzór stanowi **załącznik nr 4 do Polityki**. Jeśli zdarzenie ma charakter przestępstwa sprawa kierowana jest do organów ścigania.

W O J T
inż. Czesław Jurga

Załącznik nr l
do Polityki Bezpieczeństwa
Urzędu Gminy Czarnia

Czarnia, dn.....

(imię i nazwisko pracownika)

(adres)

Oświadczenie
(wzór)

1. l. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
   a) o ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową,
   b) o zasadach ochrony oraz środkach i zabezpieczeniach danych osobowych (Dz. U. Nr 133 poz. 833) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 28 kwietnia 2004 roku (Dz. U. Nr 100 poz. 1024 z 2004 r.) oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/ zapoznałam* się z racji wykonywanej pracy w Urzędzie Gminy Czarnia, a w szczególności nie będę:
   a) ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją technologiczną.

(podpis pracownika) (podpis przełożonego)

* niepotrzebne skreślić

Załącznik nr 2
do Polityki Bezpieczeństwa
Urzędu Gminy Czarnia

Wykaz

osób, które zostały zapoznane z „Polityką bezpieczeństwa Urzędu Gminy Czarnia" przeznaczoną dla osób zatrudnionych przy przetwarzaniu danych osobowych.

(wzór)

l/p	Nazwisko i imię	Stanowisko	Data	Podpis

Załącznik nr 4
do Polityki Bezpieczeństwa
Urzędu Gminy Czarnia

Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Czarnia

(wzór)

Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

5. Przyczyny wystąpienia zdarzenia:

6. Podjęte działania:

7. Postępowanie wyjaśniające:

(data, podpis Administratora bezpieczeństwa informacji)

Załącznik nr 2 do
Zarządzenia nr 5/2012
Wójta Gminy Czarnia
z dnia 01 marca 2012 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarnia

Podstawa prawna

§1

Paragraf 3 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w 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).

Postanowienia ogólne

§2.

1. Ilekroć mowa w niniejszym dokumencie o Instrukcji, należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarnia".
2. Ilekroć mowa w niniejszym dokumencie o Urzędzie należy przez to rozumieć Urząd Gminy Czarnia.

Zagadnienia organizacyjne

§3.

1. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się z treścią Instrukcji i jej przestrzegania.
2. Fakt zapoznania się z Instrukcją pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi **załącznik nr 1 do Instrukcji**.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

§4.

Przed rozpoczęciem pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. W

przypadku ich wykrycia należy niezwłocznie powiadomić o tym fakcie Administratora bezpieczeństwa informacji.

2. W celu rozpoczęcia pracy użytkownik wykonuje logowanie do systemu używając nadanego loginu i hasła.
3. Podczas nieobecności przy stanowisku komputerowym należy wylogować się z sytemu bądź uruchomić wygaszacz ekranu chroniony hasłem.
4. Po zakończeniu pracy w systemie należy wylogować się z sytemu i wyłączyć stację roboczą.
5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest uprzedzone informacją do pracowników Urzędu (w formie wiadomości e-mail lub osobiście) przez Administratora systemu na co najmniej 30 minut przed planowanym zawieszeniem.

Nadawanie uprawnień

§5.

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, którego wzór stanowi **załącznik nr 2 do Instrukcji**.
2. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym Urzędu nadaje Administrator danych.
3. Za rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym odpowiada Administrator systemu.
4. Administrator systemu nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez Administratora danych.

Zabezpieczenia

§6.

1. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
2. Hasła do systemu stacji roboczych kontrolowanych przez kontroler domeny (PDC) mają długość przynajmniej 10 znaków (co najmniej litery i cyfry) i okres ważności ustawiony na nie dłużej niż 2 miesiące.
3. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Za okresową (przynajmniej raz na 2 miesiące) zmianę haseł odpowiada użytkownik oprogramowania.
4. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym

przetwarzane są dane osobowe. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

Procedury tworzenia kopii zapasowych

§7.

Dane systemów kopiowane są w trybie tygodniowym (pn.-pt. kopie baz danych; pn.-pt. kopia awaryjna systemu serwera). Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie po zakończeniu pracy. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane.

Kopie zbiorów umieszczonych na serwerze wykonywane są automatycznie dedykowanym oprogramowaniem wytworzonym we własnym zakresie.

Dodatkowe kopie wynikające z np. zmiany platformy sprzętowej przechowywane są w raz z poniższymi.

Kopie awaryjne są przechowywane w szafie metalowej w pok. nr 10 Urzędu. Osobą odpowiedzialną za wymianę kopii awaryjnych na aktualne jest Administrator systemu.

Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza Administrator systemu.

Odnotowywanie udostępnienia danych

§8.

1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
   1) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   2) operacje wykonywane na przetwarzanych danych,
   3) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
   4) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   5) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
2. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

1) identyfikatora osoby, której dane dotyczą,
2) osoby przesyłającej dane,
3) odbiorcy danych,
4) zakresu przekazanych danych osobowych,
5) daty operacji,
6) sposobu przekazania danych.

Procedury wykonywania przeglądów i konserwacji systemów

§9.

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Urzędu lub przez upoważnionych przedstawicieli wykonawców.
2. Prace wymienione w ust. l powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Przed rozpoczęciem prac wymienionych w ust. l przez osoby niebędące pracownikami Urzędu należy dokonać potwierdzenia tożsamości tychże osób.

Niszczenie wydruków i nośników danych

§10.

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
2. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora bezpieczeństwa informacji.
3. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać, itp.).
4. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarce.

WÓJT
inż. Czesław Jurga

Załącznik nr 1
do Instrukcji zarządzania
systemem informatycznym
służącym do przetwarzania
danych osobowych
w Urzędzie Gminy Czarnia

Wykaz

osób, które zostały zapoznane z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarnia" przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.

(wzór)

Lp.	Nazwisko i imię	Stanowisko	**Data**	**Podpis**

Załącznik nr 2 do Instrukcji
zarządzania systemem
informatycznym służącym do
przetwarzania danych osobowych
w Urzędzie Gminy Czarnia

Czarnia, dnia.....

Upoważnienie
(wzór)

Na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926, ze zmianami) Administrator danych Urzędu Gminy Czarnia upoważnia Pana/Panią*:

do przetwarzania danych osobowych, dotyczących:

Administrator danych zobowiązuje Pana/Panią* do przestrzegania „Polityki bezpieczeństwa Urzędu Gminy Czarnia" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarnia".

Administrator danych Urzędu Gminy Czarnia

niepotrzebne skreślić