ZARZĄDZENIE Nr 122/2009

Wójta Gminy Bądkowo

z dnia 22 grudnia 2009 roku

w sprawie:

1). **instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Bądkowo**

2). **wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Bądkowo**

Na podstawie § 3 ust. 3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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) zarządza się, co następuje:

§ 1.

Wprowadza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Bądkowo", zwaną dalej instrukcją. Treść instrukcji zawiera załącznik nr 1 do zarządzenia.

§ 2.

Wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Bądkowo". Treść polityki bezpieczeństwa zawiera załącznik nr 2 do zarządzenia.

§ 3.

Zobowiązuje się wszystkich pracowników przetwarzających dane osobowe do podpisania upoważnień zezwalających na przetwarzanie danych osobowych – załącznik nr 3 do niniejszego Zarządzenia.

§ 4.

Z treścią instrukcji oraz polityki bezpieczeństwa Kierownicy referatów (równorzędnych komórek organizacyjnych) zapoznają pracowników zatrudnionych przy przetwarzaniu danych osobowych.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

Zaremba

Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym są dokumentami wewnętrznymi Urzędu Gminy i nie stanowią informacji publicznej w rozumieniu art. 1 ust. 1 ustawy z dnia 6 września 2005 roku o dostępie do informacji publicznej (Dz. U. z 2001 roku Nr 112, poz. 1198 z późn. zm.). W związku z powyższym, ze względu na interes ochrony informacji o zabezpieczeniach stosowanych w urzędzie gminy, dokumenty te nie podlegają publikacji.

Wójt

mgr Jerzy Zaremba

Załącznik nr 1 do zarządzenia nr 122
Wójta Gminy Bądkowo
z dnia 22 grudnia 2009 r.

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

§ 1.

Instrukcja określa:

1). procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności;

2). stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3). procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4). procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania;

5). sposób, miejsce i okres przechowywania:

a). elektronicznych nośników informacji zawierających dane osobowe,

b). kopii zapasowych określonych w pkt 4;

6). sposób postępowania w przypadku naruszenia ochrony danych osobowych;

7). sposób odnotowania informacji o udostępnionych danych osobowych;

8). zasady wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych;

9). zasady użytkowania sieci komputerowej.

§ 2.

Ilekroć w instrukcji jest mowa o:

1). zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

2). systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

3). administratorze danych osobowych - rozumie się przez to Wójta Gminy Bądkowo;

4). administratorze systemu informatycznego – rozumie się przez to osobę lub osoby upoważnione przez administratora danych osobowych do administrowania i zarządzania systemem informatycznym w Urzędzie Gminy Bądkowo;

5). identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

6). haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

7). publicznej sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

8). Urzędzie – rozumie się przez to Urząd Gminy Bądkowo;

9). administratorze dostępu do Internetu - rozumie się przez to osobę przygotowującą i wdrażającą koncepcję podłączenia sieci lokalnej do Internetu, administrującą serwerem i innymi urządzeniami wykorzystanymi w realizacji dostępu do Internetu;

10).Administratorze bezpieczeństwa informacji – rozumie się osobę lub osoby upoważnione i odpowiedzialne za przestrzeganie ustawy o ochronie danych osobowych.

11). Sieć lokalna należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniuy urządzeń i sieci telekomunikacyjnych.

§ 3.

1). Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie wydane przez Wójta Gminy Bądkowo.

2). Ewidencję upoważnień, o których mowa w pkt. 1, prowadzi administrator bezpieczeństwa informacji.

§ 4.

1). Upoważnienie, o którym mowa w § 3 pkt. 1, stanowi podstawę do rejestracji użytkownika systemu informatycznego.

2). Administrator systemu rejestruje osobę w systemie na wniosek administratora bezpieczeństwa informacji.

3). Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła.

4). Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, administrator systemu ustala niepowtarzalny identyfikator i hasło.

5). Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.

6). Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. O utracie uprawnień administrator bezpieczeństwa niezwłocznie informuje administratora systemu.

7). Administrator systemu przekazując użytkownikowi identyfikator i hasło przeprowadza szkolenie użytkownika z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.

8). Administrator systemu prowadzi ewidencję użytkowników systemu informatycznego. Ewidencja użytkowników powinna zawierać:

a). nazwisko i imię;

b). identyfikator użytkownika;

c). stanowisko;

d). referat, w którym użytkownik jest zatrudniony lub samodzielne stanowisko;

e). wskazanie zbiorów danych, do których użytkownik ma prawo dostępu;

f). zakres uprawnień do systemu informatycznego;

g). datę przyznania uprawnień;

h). datę wyrejestrowania użytkownika z systemu informatycznego w przypadku, gdy upoważnienie traci ważność.

§ 5.

1). Dane osobowe przetwarzane są w Urzędzie Gminy Bądkowo w sieci lokalnej za pomocą komputerów stacjonarnych.

2). Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane co 30 dni. Administrator systemu zmienia hasła lub wymusza w systemie zmianę haseł użytkowników.

3). Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić identyfikatora, hasła i stanowiska roboczego osobom nieuprawnionym.

4). Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie jego ważności.

5). Zapasowe hasła administratora systemu powinny znajdować w zabezpieczonej kopercie w sejfie Urzędu.

6). Pojedyncze komputery, na których dane osobowe służą do edycji powinny być zabezpieczone hasłem. Pracownicy zatrudnieni przy ich obsłudze nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym.

§ 6.

Każdy, kto ma uzasadnione przypuszczenie o popełnieniu przestępstwa, bądź wykroczenia przeciw ochronie danych osobowych jest obowiązany do niezwłocznego poinformowania o tym fakcie administratora bezpieczeństwa informacji, osoby przez niego wyznaczonej lub innego przełożonego w jednostce organizacyjnej. Zatajanie tych informacji lub utrudnianie postępowania wyjaśniającego stanowi poważne naruszenie obowiązków pracowniczych wraz ze wszelkimi konsekwencjami wynikającymi z obowiązujących unormowań prawnych.

Każda informacja o naruszeniu systemu bezpieczeństwa, pochodząca z któregokolwiek źródła, wymaga od administratora bezpieczeństwa informacji wszczęcia postępowania wyjaśniającego - wzór Raportu z naruszenie bezpieczeństwa danych osobowych stanowi załącznik Nr1 do Instrukcji zarządzania systemem informatycznym, aby określić:

a) czas naruszenia systemu zabezpieczeń,
b) charakter,
c) miejsce,
d) sposób,
e) skutki,
f) w jaki sposób usunąć i/lub zminimalizować skutki,
g) jakie dodatkowe środki należy zastosować w celach profilaktycznych,
h) sprawcę i cel, gdy istnieje ku temu możliwość.

Naruszenie systemu zabezpieczeń może mieć charakter:

a) wewnętrzny lub zewnętrzny,

b) incydentalny lub chroniczny,

c) nieświadomy lub zamierzony.

Miejscem zagrożenia bezpieczeństwa systemu może być:

a) strefa przetwarzania zasobów,

b) sprzęt komputerowy i inne urządzenia wykorzystywane przy przetwarzaniu,

c) oprogramowanie systemowe, sieciowe i użytkowe,

d) zawartość baz danych, rejestrów, ewidencji i innych dokumentów.

Sposób naruszenia bezpieczeństwa to:

a) osłabienie odporności systemu zabezpieczeń, w szczególności tworzenie potencjalnych zagrożeń dla systemu (np. niezamykanie pomieszczeń i/lub sejfów, pozostawianie dokumentacji i lub dostępu do aplikacji na opuszczonym stanowisku pracy albo wynoszenie poza chronioną strefę, samowolna instalacja niedozwolonych programów i/lub sprzętu na lokalnych stanowiskach pracy, itp.).

b) nieuprawnione "przeglądanie", sporządzanie notatek, wyciągów, raportów, kopii, itp..

c) zmiana zawartości zgromadzonych danych naruszająca ich integralność i/lub wiarygodność.

d) usunięcie części danych lub ich uszkodzenie,

e) fizyczne zniszczenie zasobów, kradzież sprzętu i/lub oprogramowania.

f) przekazywanie zgromadzonych danych osobom nieuprawnionym do ich posiadania.

Następstwami naruszenia systemu bezpieczeństwa mogą być:

a) stworzenie warunków zagrożenia bezpieczeństwa zasobów.

b) utrata wiarygodności i spójności informacji zawartych w bazach danych.

c) utrudnianie lub uniemożliwienie realizacji przetwarzania zasobów.

d) udostępnienie danych osobom nieupoważnionym,

e) wykorzystanie danych osobowych do celów innych niż określa ustawa upoważniająca do ich gromadzenia i przetwarzania,

f) naruszenie dóbr osobistych osób, których dane zawarte są w prowadzonych bazach.

g) narażenie na straty finansów publicznych.

Naruszenie systemu zabezpieczeń należy rozpatrywać w dwóch aspektach, wymagających odmiennych działań administratora bezpieczeństwa informacji. Tok postępowania jest uzależniony od tego, czy w następstwie zakłócenia ochrony danych osobowych zostały one ujawnione osobie nieuprawnionej. W takim przypadku należy niezwłocznie powołać komisję dla pełnego zbadania przyczyn i skutków przestępstwa, ustalenia , sprawcy i stopnia jego winy oraz wielkości poniesionych strat. Jest to podstawą zarówno do wszczynania

postępowania wobec winnych jak i minimalizacji i/lub napraw poniesionych szkód, a także działań eliminujących tego typu zdarzenia w przyszłości. Tryb ten obowiązuje również w razie stwierdzenia świadomego uszkodzenia, zniszczenia bądź bezzasadnej modyfikacji zasobów, nawet wówczas, gdy nie zostały one udostępnione osobom nieuprawnionym do ich posiadania. Zakończeniem postępowania wyjaśniającego jest sporządzenie protokołu podpisanego przez członków komisji. Postępowanie w pozostałych wypadkach nie wymaga powoływania komisji. Decyzję w tym zakresie podejmuje administrator bezpieczeństwa informacji. W razie niewielkich strat wystarczą rutynowe działania służb informatycznych pozwalające na usunięcie awarii przez serwis, odtworzenie uszkodzonych zasobów, pouczenie użytkownika, ponowna analiza systemu zabezpieczeń i ich poprawienie. Zdarzenie takie powinno być odnotowane w dzienniku pracy systemu, a po usunięciu winno zostać skontrolowane przez administratora bezpieczeństwa informacji i fakt ten także powinien zostać odnotowany.

Poważniejsze uszkodzenia struktur danych wynikające z błędów aplikacji wymagają podjęcia szybkich działań przez analityków i programistów aplikacji oraz zastosowania doraźnych działań eliminujących źródła awarii, o których każdorazowo należy powiadamiać administratora bezpieczeństwa informacji i które powinny także zostać odnotowane w dzienniku pracy systemu.

§ 7.

Dane osobowe są przetwarzane z użyciem systemu informatycznego w godzinach pracy Urzędu Gminy Bądkowo; poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu pisemnej zgody administratora bezpieczeństwa informacji, z zachowaniem warunków określonych w Regulaminie pracy Urzędu.

§ 8.

1). Ekrany monitorów stanowisk, na których przetwarzane są dane osobowe, powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
2). W pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień, o których mowa w § 3 pkt. 1, monitory stanowisk na których przetwarzane są dane osobowe powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
3). Użytkownik ma obowiązek wylogowania się z systemu przy rozpoczęciu dłuższej nieobecności na stanowisku pracy lub zakończeniu tej pracy. Stanowisko

komputerowe z uruchomionym systemem nie może pozostać bez kontroli pracującego na nim pracownika.

4). Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby nieuprawnione. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 9.

1). Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

2). Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 10.

1). Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:

a). urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej;

b). sporządzania kopii zapasowych zbiorów danych.

2). Kopie zapasowe baz danych zainstalowanych na serwerze Urzędu – wykonuje się codziennie na dysku lokalnym oraz co 30 dni na zewnętrznym dysku. W przypadku baz danych zainstalowanych na komputerach lokalnych kopię raz na 30 dni wypala się na CDR.

3). Za wykonywanie kopii, o których mowa w pkt. 2, odpowiedzialny jest administrator systemu. W przypadku zbiorów danych przetwarzanych lokalnie za wykonanie bieżących kopii zapasowych zbiorów danych odpowiedzialny jest użytkownik wyznaczony do wykonania tego zadania przez swojego przełożonego.

4). Administrator systemu nie ma obowiązku sporządzania kopii zapasowej, jeżeli w danym dniu nie wykonano zapisu zmieniającego bazę danych.

5). Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu. Nośniki danych po

ustaniu ich użyteczności należy pozbawiać danych lub niszczyć w sposób uniemożliwiający ich odczyt.

6). Kopie zapasowe miesięczne należy przechowywać w kasie pancernej Urzędu. Kopie baz danych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w pomieszczeniach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

7). Kopie miesięczne przechowuje się przez okres 3 miesięcy. W przypadku danych księgowych okres przechowywania danych wynosi 5 lat.

§ 11.

1). W związku z istnieniem zagrożenia dla zbiorów danych ze strony wirusów komputerowych oraz oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.

2). Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych:

   a). serwery, programy i zbiory danych zainstalowane na serwerach, nośniki informacji będące w bezpośrednim użytkowaniu przez administratora systemu winny być sprawdzane przez administratora systemu na obecność wirusów komputerowych co najmniej raz w tygodniu lub w razie potrzeby częściej;

   b). komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego. Użytkownik komputera, w którym jest zainstalowany program antywirusowy zobowiązany jest do sprawdzenia komputera raz w tygodniu na obecność wirusów komputerowych oraz co 3 dni do dokonania aktualizacji bazy wirusów tego programu w przypadku, gdy aktualizacja automatyczna nie działa.

3). Przeciwdziałanie zagrożeniom, które są związane z podłączeniem sieci lokalnej z publiczną:

   a). serwer i inne urządzenia wykorzystywane w realizacji dostępu do Internetu posiadają oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem do sieci lokalnej;

   b). administrator dostępu do Internetu monitoruje na bieżąco stan bezpieczeństwa, analizuje logi pod kątem naruszenia zabezpieczeń; raz na tydzień dokonuje szczegółowej analizy stanu zabezpieczeń.

§ 12.

Użytkownik zapisuje w programie informację o odbiorcach danych osobowych, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, jeżeli system informatyczny nie jest używany do przetwarzania danych zawartych w zbiorach jawnych.

§ 13.

1). Przeglądy i konserwacje systemu i zbiorów danych wykonuje administrator systemu na bieżąco, lecz nie rzadziej niż raz w miesiącu. Administrator sprawdza spójność danych, indeksów oraz stan nośników np. dysków twardych.
2). Administrator systemu okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.

§ 14.

Urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe należy pozbawić tych danych przed ich przekazaniem innemu podmiotowi. Nośniki danych zawierające dane osobowe są likwidowane poprzez uszkodzenie w sposób uniemożliwiający ich odczytanie. Naprawę wymienionych urządzeń należy wykonać pod nadzorem osoby upoważnionej przez administratora danych lub jeśli jest to możliwe, pozbawić je danych osobowych przed wydaniem ich do naprawy.

§ 15.

Korzystającym z systemu informatycznego w Urzędzie zabrania się:

1). udostępniania stanowiska pracy oraz istniejących w nich danych osobom nieupoważnionym;
2). udostępniania osobom nieuprawnionym programów komputerowych;
3). używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna;
4). przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne;
5). samowolnego instalowania i używania programów komputerowych; programy komputerowe instalowane są przez administratora systemu lub za jego zgodą przez inną upoważnioną osobę;
6). używania nośników danych udostępnionych przez osoby nieuprawnione;

7). używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy te nośniki przeskanować programem antywirusowym; jeżeli program antywirusowy nie jest zainstalowany na danej stacji roboczej należy to zrobić na innym stanowisku;

8). wykorzystywania sieci komputerowej w celach innych, niż wyznaczone przez administratora danych osobowych.

Załącznik Nr 3

do Zarządzenia nr 122
z dnia 22.12.2009r

U P O W A Ż N I E N I E

imienne do przetwarzania danych osobowych

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002r. Nr 101, poz. 926, z późniejszymi zmianami) Administrator Danych Urzędu Gminy Bądkowo – Janusz Zaremba.

upoważnia Pana/Panią .....
zatrudnioną (ego) w .....
na stanowisku .....

do przetwarzania danych osobowych, dotyczących mieszkańców gminy Bądkowo w zakresie.....
i nadaje identyfikator: .....

Administrator Danych zobowiązuje Pana/Panią do zachowania w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczania.

.....
podpis

Oświadczam, że zapoznałam/em się z „Polityką Bezpieczeństwa Informacji" i „Instrukcją Zarządzania Systemem Informatycznym" a także innymi dokumentami regulującymi zasady przetwarzania danych osobowy. Ponadto zobowiązuję się do zachowania w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczania.

.....
podpis

Załącznik nr 1
do Instrukcji zarządzania
systemem zabezpieczeń

Raport o naruszeniu danych osobowych

Sporządzający raport:
Imię i nazwisko .....
stanowisko (funkcja) .....
Dział, pokój ,nr telefonu .....

Kod formy naruszenia ochrony danych ..... (wg tabeli)
1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):
.....
.....
2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):
.....
.....
.....
3) Osoby , które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:
.....
.....
.....
4) Informacje o danych, które zostały lub mogły zostać ujawnione:
.....
.....
.....
.....
5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:
.....
.....
.....
6) Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):
.....
.....
.....
.....

Data: ..... Podpis: .....

Tabela form naruszeń danych osobowych

Nr (kod) naruszeń	Formy naruszeń	Sposób postępowania
A	**Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych**	
A.1	**W zakresie wiedzy:**	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić administratora bezpieczeństwa informacji.
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić administratora bezpieczeństwa informacji.
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić administratora bezpieczeństwa informacji.
A.2	**W zakresie sprzętu i oprogramowania**	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymieniona czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
A.2.6	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
A.2.7	Odczytywanie dyskietek i innych nośników	Pouczyć osobę popełniającą wymienioną

	przed sprawdzeniem ich programem antywirusowym.	czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
A.3	**W zakresie dokumentów i obrazów zawierających dane osobowe.**	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń sporządzić raport.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
A.4	**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych**	
A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych . Sporządzić raport.
A.4.2	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i administratora bezpieczeństwa informacji. Sporządzić raport.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.

A.5	**W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci.**	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
B	**Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych.**	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie administratora bezpieczeństwa informacji oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie administratora bezpieczeństwa informacji. Sporządzić raport.
C	**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem**	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.

Załącznik nr 2 do zarządzenia Nr 122
Wójta Gminy Bądkowo
z dnia 22 grudnia 2009 r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Bądkowo

§ 1.

1. Polityka bezpieczeństwa określa:
   1). wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
   2). wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
   3). opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   4). sposób przepływu danych pomiędzy poszczególnymi systemami;
   5). środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
2. Polityka bezpieczeństwa dotyczy zabezpieczania danych osobowych przetwarzanych tradycyjnie i w systemach informatycznych w Urzędzie Gminy Bądkowo.

§ 2.

Ilekroć w polityce bezpieczeństwa jest mowa o:
1). danych osobowych rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
2). zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów - są to:
   - dokumentacje papierowe (korespondencja, wnioski, deklaracje,itp),
   - systemy informatyczne przetwarzania danych osobowych oraz oprogramowanie komputerowe służące do przetwarzania informacji,
   - wydruki;
3). przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, zmienianie, udostępnianie i usuwanie;

4). systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

5). poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

6). integralności danych – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

7). rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane tylko temu podmiotowi;

8). administratorze danych – rozumie się przez to Wójta Gminy Bądkowo.

9). administratorze bezpieczeństwa informacji – rozumie się przez to pracownika urzędu lub inną osobę wyznaczoną przez administratora danych do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresiue ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

10). administratorze systemu – rozumie się przez to osobę lub osoby upoważnione przez administratora danych osobowych do administrowania i zarządzania systemem informatycznym na terenie Urzędu Gminy Bądkowo oraz stosowania technicznych i organizacyjnych środków ochrony.

§ 3.

1) Obszar, w którym przetwarzane są dane osobowe tworzy jeden budynek Urzędu Gminy Bądkowo przy ul. Włocławskiej 82.

2) Wykaz pomieszczeń, w których przetwarzane są dane osobowe prowadzi administrator bezpieczeństwa informacji.

3) Wykaz pomieszczeń, w których przetwarzane są dane osobowe:

- parter:
  - Serwerownia
  - Referat finansowo – budżetowy (pok. nr.2,3,4,5.6)
  - Referat Obsługi Rolnictwa (pok.7)
  - Gminny Ośrodek Pomocy Społecznej (pok.1)
  - Kancelaria tajna

- piętro:
    - Działalność gospodarcza, spawy wojskowe, obrona cywilna, zarządzanie kryzysowe (pok. nr 14)
    - Ewidencja ludności, dowody osobiste, USC (pok. nr 12)
    - Sekretarz Gminy (pok. nr.11)
    - Kadry i płace (pok. nr 13)
    - Sekretariat, biuro Rady Gminy, sprawy kancelaryjne (pok. Nr 9)
    - Wójt Gminy (pok.nr.10)
- poddasze:
    - Archiwum

§ 4.

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych w zbiorach:

1) Ewidencja ludności

Program: Ewidencja firmy Radix

Lokalizacja zbioru: Stanowisko ds. ewidencji ludności (piętro budynku pok.nr 12)

Struktura zbioru: dane ewidencyjne: imiona, nazwisko, data urodzenia, nazwisko rodowe, imiona i nazwiska rodowe rodziców, adres stały, adres czasowy, stan cywilny, dokument tożsamości, rysopis (wzrost, kolor oczu),miejsce urodzenia, nr aktu urodzenia,miejsce zawarcia związku małżeńskiego, -nr aktu, data, , seria i nr książeczki wojskowej, sdtopień wojskowy, uprawnienia wyborcze, wykształcenie, imię i nazwisko współmałżonka, dane dotyczące zgonu, poprzednie adresy czasowe, poprzednie adresy stałe, poprzednie dokumenty tożsamości, poprzednie nazwiska, poprzednie imiona, poprzednie stany cywilne, obywatelstwo, narodowość, adnotacje o rozwodzie, obowiązek wojskowy, numer ewidencyjny PESEL, adresy byłych mieszkańców

2) Dowody osobiste

Program: IDL SYSTEM

Lokalizacja zbioru: stanowisko ds. dowodów osobistych (piętro budynku, pok. Nr 12)

Struktura zbioru: imiona i nazwisko, data urodzenia, nazwisko rodowe, imiona i nazwisko rodowe rodziców, miejsce urodzenia adres zamieszkania, rysopis (wzrost, kolor oczu) numer PESEL, płeć, rodzaj zameldowania, kod pocztowy, posiadany dotychczasowy dokument tożsamości (seria, nr, nazwa i siedziba wystawcy),

przyczyna wystawienia dowodu, data i przyczyna utraty, podpis osoby, fotografia (wizerunek twarzy)

3) **Księgi Stanu Cywilnego**

Prowadzone są metodą tradycyjną - ręczną

lokalizacja zbioru: Stanowisko samodzielne USC (pok. Nr 12)

Struktura zbioru:

Dane do aktu urodzenia: dane dotyczące dziecka: nazwisko, imię (imiona), data urodzenia, miejsce urodzenia, płeć

dane dotyczące rodziców: nazwiska, imiona, nazwiska rodowe, daty urodzenia, miejsce urodzenia, miejsce zamieszkania, zawód, numer aktu

dane dotyczące zgłaszającego urodzenie: nazwisko i imię, miejsce zamieszkania

Dane do aktu małżeństwa: imię(imiona), nazwisko, nazwisko rodowe, stan cywilny, data urodzenia i miejsce zamieszkania, data i miejsce zawarcia związku małżeńskiego.

Dane dotyczące rodziców: imiona, nazwisko, nazwisko rodowe, nazwisko noszone po zawarciu związku małżeńskiego, imiona i nazwisko świadków,

Dane do aktu zgonu: dane dotyczące małżonka osoby zmarłej: nazwisko i imię, nazwisko rodowe

dane dotyczące rodziców osoby zmarłej: imiona, nazwiska rodowe

dane dotyczące osoby zgłaszającej zgon: nazwisko i imię, adres, nr PESEL,

4) **Ewidencja podatników**

Program: PODATKI. KSZOB (księgowość zobowiązań) firmy INFO-SYSTEM

lokalizacja zbioru: Referat finansowo – budżetowy (parter pok.2, 3.4,5,6), dane w serwerze

struktura zbioru :

podatnicy podatku od nieruchomości osób fizycznych: imię i nazwisko, adres, nr NIP, nr REGON, rodzaj własności

podatnicy podatku od nieruchomości osób prawnych:

podatnicy podatku rolnego , leśnego: imię i nazwisko, adres , nr NIP, nr REGON, rodzaj własności

podatnicy podatku od posiadania psów: imię i nazwisko, adres, nr NIP, nr REGON, rodzaj własności

podatnicy podatku od środków transportowych: imię i nazwisko, adres, nr NIP , nr REGON, rodzaj własności

podatnicy z tytułu odprowadzenia ścieków: imię i nazwiska,adres, nr NIP,

ewidencja gruntów i budynków – imię i nazwisko, PESEL, NIP, nr działki, powierzchnia, numer obrębu, numer jednostki rejestrowej, numer księgi wieczystej, identyfikator działki ewidencyjnej;

akcyza – imię i nazwisko, adres, PESEL, rodzaj dokumentu stwierdzającego tożsamość, pow. użytków rolnych;

Księgowość

Program: HomE – banking KBS Aleksandrów Kujawski

lokalizacja zbioru: referat finansowo – budżetowy (pok.2, 3,4,5)

dokonywanie przelewu - struktura zbioru: nazwisko i imię, nazwa firmy, adres, numer rachunku końcowego.

5) **KASA**

program KASA firma INFO – SYSTEM

Lokalizacja zbioru: Referat finansowo-budżetowy (Kasa), dane w serwerze

struktura zbioru: imię i nazwisko, adres zamieszkania, NIP, PESEL, imię ojca, imię matki, numer konta

6) **Woda**

Program Wodnik firmy INFO-SYSTEM

Lokalizacja zbioru: Referat Finansowo-budżetowy, dane w serwerze

Struktura zbioru imię i nazwisko, adres zamieszkania,

7) **Użytkownicy wieczyści, dzierżawcy, najemcy**

Prowadzone są metodą tradycyjną ręcznie

Lokalizacja zbioru: Referat obsługi Rolnictwa

Struktura zbioru: imię i nazwisko, adres zamieszkania, seria i numer dowodu osobistego, nr NIP, numer położenia nieruchomości,

8) **Ochrona środowiska**

Program: EDOŚ firmy ARISCO

Lokalizacja zbioru : Referat Obsługi Rolnictwa (parter pok.nr 7)

Struktura zbioru: imię i nazwisko, adres, lokalizacja nieruchomości,

Ewidencja danych o dokumentach zawierających informacje o środowisku i jego ochronie.

9) **Dodatki mieszkaniowe**

Program: System obsługi jednostek budżetowych firmy CHEOPS

Lokalizacja zbioru : Stanowisko ds dodatków mieszkaniowych (parter pok.nr 1 siedziba GOPS)

Zakres informacji gromadzonych w danym zbiorze : nazwisko i imię, nr PESEL, data urodzenia, adres zamieszkania wnioskodawcy.

10) Świadczenia rodzinne

Program: SR świadczenia rodzinne Sygnity SYRGIUSZ

Lokalizacja zbioru

Budynek UG GOPS, Stanowisko ds świadczeń rodzinnych.

Struktura zbioru: nazwisko i imię, nr PESEL, nr NIP, stan cywilny, obywatelstwo, miejsce zamieszkania wnioskodawcy. Nazwisko i imię, stopień pokrewieństwa, nr PESEL członków rodziny wnioskodawcy.

11) Przydział lokalu z gminnego zasobu mieszkaniowego

Program: zbiór prowadzony w formie tradycyjnej - papierowej

Lokalizacja zbioru: Referat ROR (parter pok. Nr 7)

Struktura zbioru i zakres informacji przetwarzanych w danym zbiorze:

Dane dotyczące wszystkich osób zamieszkałych z wnioskodawcą - imiona i nazwiska, stosunek do wnioskodawcy (członek rodziny, obcy), data zameldowania (na pobyt stały, czasowy),

Dane osób ubiegających się o przydział mieszkania – jw oraz stosunek pokrewieństwa do wnioskodawcy, wysokość wynagrodzenia, rodzaj wykonywanej pracy.

12) Przeciwdziałanie alkoholizmowi

Program: zbiór prowadzony w formie tradycyjnej – papierowej

Lokalizacja zbioru: stanowisko ds profilaktyki i przeciwdziałania alkoholizmowi (budynek UG w GOPS pok. Nr 1)

Struktura zbioru i zakres informacji przetwarzanych w danych zbiorze:

Dane dotyczące osoby, wobec której prowadzi się postępowanie w sprawie skierowania na badania przez biegłego w celu wydania opinii w przedmiocie uzależnienia od alkoholu i wskazania rodzaju zakładu leczniczego - Imię , nazwisko, miejsce zamieszkania , informacje z wywiadu przeprowadzanego przez policję (stan rodzinny, stosunek do rodziny praca, nadużywanie alkoholu, zakłócenie spokoju i porządku publicznego) , informacje z wywiadu środowiskowego pracownika socjalnego dotyczące rodziny i sytuacji materialnej,

Dane dotyczące rodziny: imiona i nazwiska, stosunek pokrewieństwa, informacja o nauce/pracy

Dane osobowe dzieci zakwalifikowanych na obóz socjo-terapeutyczny i uczestniczących w działaniach profilaktycznych – imię, nazwisko,data urodzenia,adres, sutuacja rodzinna,

13) Kadry PŁACE Urzędu

Program : Płatnik – instalacja stanowisko ds. kadr i płac, firma INFO - SYSTEM

Lokalizacja zbioru: UG piętro pok.nr 13, dane w serwerze

Struktura zbioru: imię i nazwisko adres, nr telefonu, NIP, PESEL, data urodzenia, miejsce urodzenia, imiona rodziców, nazwisko rodowe, nazwisko rodowe matki, wykształcenie, świadectwo pracy, stan cywilny, imiona dzieci i małżonka, ich daty urodzenia i PESEL.

14) Akta osobowe pracowników

Program; zbiór prowadzony w formie tradycyjnej

Struktura zbioru: j.w.

15) Kandydaci do pracy w Urzędzie

Program: zbiór prowadzony w formie tradycyjnej

Lokalizacja zbioru: piętro budynku UG pok.nr 13

Struktura zbioru: imię i nazwisko adres, nr telefonu, data urodzenia, stan cywilnego, wykształcenie, kwalifikacje, doświadczenie zawodowe.

16) Archiwum zakładowe

Program: zbiór prowadzony w formie tradycyjnej – papierowej

Lokalizacja zbioru: poddasze - budynek UG

17) Rejestracja i kwalifikacja wojskowa

Program: zbiór prowadzony w formie tradycyjnej – papierowej

Lokalizacja zbioru: budynek UG piętro pok. Nr 14

Dane dotyczące osób rejestrowanych i kwalifikowanych - nazwisko i imię, imię ojca, data urodzenia , seria i numer dowodu osobistego, miejsce aktualnego pobytu (stałego, czasowego), nr książeczki wojskowej

18) Stypendia szkolne

Program: STYPENDIUM.NET firmy INTERNET COMMUNITY

Lokalizacja zbioru: piętro UG pokój nr 15- GZEASz

Struktura zbioru: dane dotyczące ucznia ubiegającego się o pomoc materialną o charakterze socjalnym – imię, nazwiska, adres zamieszkania , nr PESEL., imię i

nazwisko opiekuna prawnego wnioskującego o stypendium dla ucznia, adres miejsce nauki,

dane wnioskodawcy – imię i nazwisko, adres zamieszkania, PESEL, dochód na osobę, dokument tożsamości.

19) **Decyzje o warunkach zabudowy**

Prowadzone są metodą tradycyjną

Lokalizacja zbioru – Refera obsługi rolnictwa pok. Nr 7

struktura zbioru – nazwisko i imię, adres zamieszkania. miejsce i numer położenia nieruchomości.

20) Działalność gospodarcza

Prowadzona jest metadą tradycyjną

Lokalizacja zbioru – stanowisko ds.działalności gospodarczej pok.nr 14

struktura zbioru – imię i nazwisko. miejsce zamieszkania ,adres przedsiębiorcy. siedzib i adres zakładu głównego, PESEL, NIP, nazwa pod którą wykonywana jest działalnośćgospodarcza, kod i opis przedmiotu wg.PKD, data rozpoczęcia działalności, data zakończenia działalności, data zawieszenia działaności;

2. Powyższy wykaz prowadzi Administrator Bezpieczeństwa Informacji.

§ 5.

1. W ramach procesów przetwarzania danych jest możliwość przepływu danych w ramach integracji systemów INFO – SYSTEM, zabezpieczenie jest na poziomie haseł i nazw użytkowników.
2. Sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi w sieci lokalnej Urzędu Gminy w Bądkowie:

   System PLACE - istnieje możliwość przepływu danych zbiorczych płacowych do systemu BUDŻET.

   System PODATKI- istnieje możliwość przepływu danych osobowych z systemu KSZOB, KASA. WODA. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

   Systemu PLACE - eksportowane są dane w postaci pliku, o formacie ustalonym przez

twórców programu PŁATNIK. Plik ten jest importowany przez system PŁATNIK, który służy do rozliczeń pracowników z ZUS. Transmisja danych do ZUS odbywa się przez teletransmisję, drogą jaką określił ZUS.

§ 6.

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

1. Środki ochrony fizycznej
   a). Budynek urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest zabezpieczony alarmem.
   b). Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
   c). Okna i drzwi na parterze są zabezpieczone kratami lub roletami zewnętrznymi.
   d). Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji.
   e). Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
   f). W przypadku przebywania interesantów bądź innych 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, osoba odpowiedzialna za obsługę informatyczną urzędu oraz Administrator Danych.
   h). Przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. g.

2. Środki sprzętowe, informatyczne i telekomunikacyjne

a). Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia powinien być zniszczony w sposób uniemożliwiający jego odczytanie, przy pomocy niszczarki, która umożliwia cięcie poprzeczne.

b). Na stanowiskach pracy, w których przetwarzane są dane osobowe zastosowano oprogramowanie umożliwiające tworzenie kopii zapasowych.

c). Na serwerze zainstalowano oprogramowanie antywirusowe oraz firewall.

3. Środki ochrony w ramach oprogramowania systemu

a). Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osoby zajmującej się obsługą informatyczną urzędu, Administratora Bezpieczeństwa Informacji.

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

c). System informatyczny z jakiego korzystają pracownicy urzędu gminy 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, chyba że program tego nie przewiduje – wówczas jedynym środkiem zabezpieczenia jest hasło systemowe.

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 organizacyjne

a). Wyznaczono Administratora Bezpieczeństwa Informacji, który przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia Administratora Danych osobowych określającego zakres uprawnień pracownika.

b). Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy zapoznają się z obowiązującymi przepisami o ochronie danych osobowych, procedurami przetwarzania danych oraz zagrożeniami związanymi z przetwarzaniem danych w systemie informatycznym.

c). Prowadzona jest ewidencja osób upoważnionych do przetwarzania 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.

§ 7.

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Urzędu upoważnieni do przetwarzania danych.