URZĄD GMINY
59-150 GRĘBOCICE
powiat Polkowice
woj. dolnośląskie

ZARZĄDZENIE nr 12/2007

Wójta Gminy Grębocice

z dnia 18 stycznia 2007r.

w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Grębocice

Działając na podstawie art. 36 § 2 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2004 roku nr 33 poz. 285 z późn. zm.) oraz § 3 ust. 3 Rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100 poz. 1024) zarządzam, co następuje:

§ 1

Wprowadzam:

1. **Politykę Bezpieczeństwa Urzędu Gminy Grębocice**
   - załącznik nr 1
2. **Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Grębocice**
   - załącznik nr 2.

§ 2

Wdrożenie dokumentacji wskazanej w § 1 powierzam Administratorowi Bezpieczeństwa Informacji Urzędu Gminy Grębocice.

§ 3

Kierownictwo komórek organizacyjnych Urzędu Gminy Grębocice zobowiązuję do zapoznania podległych pracowników oraz przyjęcie od każdego zapoznanego pracownika **Oświadczenia** wg wzoru stanowiącego załącznik nr 3 do niniejszego Zarządzenia.

§ 4

Pracownik Referatu Organizacyjnego zajmujący się sprawami kadrowymi Urzędu, dokument wymieniony w § 3 załączy do teczki personalnej pracownika.

§ 5

Zarządzenie wchodzi w życie z dniem 1 lutego 2007r.

WÓJT GMINY
GRĘBOCICE
mgr inż. Roman Jabłoński

URZĄD GMINY
GRĘBOCICE

POLITYKA BEZPIECZEŃSTWA

→ * ←

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

STYCZEŃ 2007

URZĄD GMINY GRĘBOCICE

Załącznik nr 1
do Zarządzenia nr 12/2007
Wójta Gminy Grębocice z dnia 18 stycznia 2007r.

Polityka Bezpieczeństwa

WPROWADZENIE

Polityka bezpieczeństwa jest podstawowym elementem regulującym zasady zapewnienia bezpieczeństwa danych osobowych w Urzędzie Gminy Grębocice.

Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy Grębocice. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu Gminy. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Administrator danych, którym jest Wójt, swoją Decyzją wyznacza **Administratora Bezpieczeństwa Informacji,** zwanego dalej ABI oraz osobę zastępującą ABI w czasie jego dłuższej nieobecności.

1) ABI realizuje zadania w zakresie ochrony danych, a w szczególności:
   - ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu Gminy Grębocice,
   - podejmowania stosownych działań zgodnie z niniejszą „Polityką Bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   - niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   - nadzoru i kontroli systemów informatycznych służących do przetwarzania danych

osobowych i osób przy nim zatrudnionych.

2) Osoba zastępująca ABI powyższe zadania realizuje w przypadku nieobecności ABI

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 roku Dz. U. Nr 101, poz. 926 z późn. zm.),
- ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (tekst jednolity z 2005 roku Dz. U. nr 196, poz. 1631),
- oraz aktów wykonawczych wydanych na podstawie ww. ustaw

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

Podział zagrożeń:

1) **zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych

2) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) **zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy).

Zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do system z jego wnętrza,
- nieuprawniony przekaz danych,
- pogorszenie jakości sprzętu i oprogramowania,
- bezpośrednie zagrożenie materialnych składników systemu.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem Danych zawartych i przetwarzanych w systemach informatycznych Urzędu Gminy Grębocice jest Wójt.

2. Administrator Danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu Gminy, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:
   1) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach
   2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1,
   3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie zaawansowanego systemu kontroli dostępu oraz zalecanego systemu ochrony p-poż. dla urządzeń elektronicznych,
   4) wyposażenie pomieszczeń w szafy metalowe dające gwarancję bezpieczeństwa dokumenttacji.

4. Do zastosowanych środków organizacyjnych należą następujące zasady:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń

i programów związanych z przetwarzaniem i ochroną danych osobowych,

3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i nie pozostawianiu pomieszczenia w czasie godzin pracy bez nadzoru

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka Bezpieczeństwa w Urzędzie Gminy Grębocice" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie. Dokumenty te nie mogą być sprzeczne z regulacjami określonymi w Polityce Bezpieczeństwa.

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator Danych – Wójt Gminy - za pośrednictwem Administratora Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z Ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. ABI sporządza półroczne plany kontroli zatwierdzone przez Wójta Gminy i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, ABI sporządza roczne sprawozdanie i przedstawia Administratorowi Danych (Wójtowi Gminy).

Rozdział 4

POSTANOWIENIA KOŃCOWE

1) Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2) Osoby, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt poprzez podpisanie oświadczenia wg wzoru stanowiącego załącznik nr 3 do Zarządzenia nr 12/2007 Wójta Gminy Grębocice z dnia 18 stycznia 2007r. wprowadzającego dokumentację przetwarzania danych osobowych. Oświadczenia takie przechowywane są w aktach personalnych pracownika w Referacie Organizacyjnym.
3) Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity z 2002 r. Dz.U. Nr 101, poz. 926 z późn. zmianami) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
4) Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w każdej innej formie.
5) Wdrożenie Polityki Bezpieczeństwa odbywa się na podstawie planu opracowanego przez ABI, który zawiera w szczególności:
   - zakres, sposób i czas zapoznania się pracowników z Polityką Bezpieczeństwa
   - terminarz szkoleń z zakresu wprowadzanych procedur
   - terminarz szkoleń stanowiskowych

- terminarz wprowadzenia do stosowania poszczególnych elementów Polityki Bezpieczeństwa
- termin kontroli stosowania wszystkich postanowień wprowadzonych Polityką Bezpieczeństwa
- sprawdzenie funkcjonowania procedur poprzez symulację jednego z zagrożeń określonych w Instrukcji postępowania w sytuacji naruszenia systemu ochrony danych osobowych
- analizę zgodności innych wewnętrznych aktów prawa z Polityką Bezpieczeństwa, a w przypadku stwierdzonych niezgodności harmonogram dostosowania ich postanowień do wymogów Polityki Bezpieczeństwa
- zestawienie zawierające potrzeby w zakresie dostosowania struktury organizacyjnej oraz stosowanego sprzętu i oprogramowania.

Wykaz załączników do Polityki Bezpieczeństwa:

1. Instrukcja w sprawie ochrony danych osobowych w systemach informatycznych - zał. Nr 1
2. Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych - zał. Nr 2
3. Wykaz baz danych w systemach informatycznych, w których przetwarzane są dane osobowe - zał. Nr 3
4. Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów - zał. Nr 4
5. Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych - zał. Nr 5
6. Ewidencja pracowników upoważnionych do przetwarzania danych osobowych - zał. Nr 6
7. Zgłoszenie zbioru danych Generalnemu Inspektorowi Danych Osobowych - zał. Nr 7
8. Opis struktury zbiorów danych - zał. Nr 8
9. Sposób przepływu danych pomiędzy poszczególnymi systemami - zał. Nr 9
10. Określenie wykorzystanych środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych - zał. Nr 10
11. Procedury awaryjne - zał. Nr 11

Załącznik **nr 1**
do **Polityki Bezpieczeństwa**

Instrukcja

w sprawie ochrony danych osobowych

Na podstawie art. 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity z 2002 roku Dz.U. nr 101 poz. 926 z późn. zm.); Rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100 poz. 1024) oraz art. 94 ust.1 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz.U. z 1998 r. nr 21 poz. 94 wraz z późn. zm.) ustalam, co następuje:

§ 1

Przetwarzanie danych osobowych pozostających w bazach danych Urzędu Gminy Grębocice i jednostek organizacyjnych Gminy Grębocice, służy realizacji zadań wynikających z Ustawy o samorządzie gminnym oraz innych zadań powierzonych.

§ 2

1. Administratorem danych w Urzędzie Gminy Grębocice w rozumieniu Ustawy o ochronie danych osobowych jest Wójt.
2. Obowiązki wynikające z Ustawy o ochronie danych osobowych Wójt powierza:
   a.) lokalnym administratorom (dyrektorzy/kierownicy jednostek organizacyjnych Gminy)
   b.) kierownikom komórek organizacyjnych
   w zakresie podległych im pracowników.

3. Obowiązki wynikające z ustawy o ochronie danych osobowych Rada Gminy Grębocice powierza lokalnym administratorom - dyrektorom/kierownikom podległych jednostek organizacyjnych, niebędących w strukturze organizacyjnej Urzędu Gminy Grębocice i zobowiązuje ich do wyznaczenia Administratora Bezpieczeństwa Informacji w podległych im jednostkach i opracowania własnej Polityki Bezpieczeństwa.

§ 3

1. Zgodnie z wymogami 36 ust. 3 ustawy Wójt Gminy Grębocice wyznacza osobę zwaną dalej „Administratorem Bezpieczeństwa Informacji", odpowiedzialną za bezpieczeństwo danych osobowych w systemach informatycznych Urzędu Gminy Grębocice.
2. Administrator Bezpieczeństwa Informacji realizuje zadania wynikające z ustawy z pomocą pracowników wymienionych w § 2 ust. 2 niniejszej instrukcji

§ 4

1. Zobowiązuje się Administratora Bezpieczeństwa Informacji do osobistego:
   a.) prowadzenia ewidencji baz danych w systemach informatycznych, w których przetwarzane są dane osobowe w Urzędzie Gminy Grębocice, zgodnie z załącznikiem nr 3 do Polityki Bezpieczeństwa,
   b.) prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów, zgodnie z załącznikiem nr 4 do niniejszej Polityki Bezpieczeństwa,
   c.) prowadzenia ewidencji miejsc przetwarzania danych osobowych i sposobu ich zabezpieczania, zgodnie z załącznikiem nr 5 do Polityki Bezpieczeństwa
   d.) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych stanowiącej załącznik nr 6 do Polityki Bezpieczeństwa.
2. Zobowiązuje się pracownika Referatu Organizacyjnego zajmującego się sprawami kadrowymi Urzędu Gminy Grębocice do uzupełniania akt osobowych pracowników zatrudnionych przy przetwarzaniu danych osobowych o oświadczenia, z których wynika, że zapoznali się z przepisami obwiązującymi w tym zakresie.
3. Udostępnianie danych osobowych pozostających w bazach danych Urzędu Gminy Grębocice do celów innych niż określone w § 1 niniejszej Instrukcji, odbywa się wyłącznie

za pośrednictwem Referatu Organizacyjnego Urzędu Gminy Grębocice, po uprzednim uzyskaniu zgody Wójta Gminy.

§ 5

Lokalni administratorzy danych osobowych zobowiązani są do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

a.) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,

b.) zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,

c.) wykonywania zaleceń Administratora Bezpieczeństwa Informacji Urzędu Gminy Grębocice w zakresie ochrony danych osobowych w funkcjonujących podległych im jednostkach systemach informatycznych,

d.) przekazywanie na bieżąco do Administratora Bezpieczeństwa Informacji zaktualizowanych danych do dokumentów sporządzonych wg załączników nr 3, 4, 5 do Polityki Bezpieczeństwa.

e.) wdrażanie i nadzorowanie przestrzegania „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych",

f.) działanie zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych" stanowiącej załącznik nr 2 do Polityki Bezpieczeństwa, stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych w podległych im jednostkach.

§ 6

Osoby nieprzestrzegające przepisów w zakresie ochrony danych osobowych podlegają, niezależnie od odpowiedzialności wynikającej z Kodeksu Pracy, sankcjom przewidzianym w rozdziale 8 Ustawy o ochronie danych osobowych.

§ 7

1. Zobowiązuje się lokalnych administratorów danych osobowych w terminie 14 dni od dnia wejścia w życie Zarządzenia wprowadzającego niniejsze dokumenty do:
   a.) przygotowania i przekazania do Administratora Bezpieczeństwa Informacji Urzędu Gminy „Wykaz baz danych w systemach informatycznych, w których przetwarzane są dane osobowe", zgodnie z załącznikiem nr 3 do Polityki Bezpieczeństwa,
   b.) przygotowania i przekazania do Administratora Bezpieczeństwa Informacji „Ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów", zgodnie z załącznikiem nr 4 do Polityki Bezpieczeństwa,
   c.) przygotowania i przekazania do Administratora Bezpieczeństwa Informacji „Wykazu miejsc, w których ma miejsce przetwarzanie danych osobowych w systemach informatycznych i sposobu ich zabezpieczania", zgodnie z załącznikiem nr 5 do Polityki Bezpieczeństwa,

   w podległych im komórkach organizacyjnych.
2. Zasady dostępu do systemu informatycznego określono w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie Gminy Grębocice, będącą załącznikiem nr 2 do Zarządzenia nr .../2007 Wójta Gminy Grębocice.

§ 8

Instrukcja dotyczy w równym stopniu przetwarzania danych w systemach innych niż informatyczne.

Załącznik **nr 2**
do **Polityki Bezpieczeństwa**

Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych

§ 1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 2

Instrukcja określa tryb postępowania w przypadku, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 3

1. **Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:**
   - **sytuacje losowe lub nieprzewidziane** oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   - **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   - **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

- **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu
- **jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego** wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- **nastąpiło naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie,
- **stwierdzono próbę lub modyfikację danych lub zmianę** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- **nastąpiła niedopuszczalna manipulacja** danymi osobowymi w systemie,
- **ujawniono osobom nieupoważnionym** dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
- **praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa** od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- **ujawniono istnienie nieautoryzowanych kont dostępu** do danych lub tzw. "bocznej furtki", itp.
- **podmieniono lub zniszczono nośniki z danymi** osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- **rażąco naruszono dyscyplinę pracy** w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)

2. Za naruszenie ochrony danych uważa się również stwierdzone 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.

§ 4

1. Każda osoba zatrudniona w Urzędzie Gminy, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), zobowiązana jest niezwłocznie poinformować o tym osobę zatrudnioną

przy przetwarzaniu danych osobowych lub Administratora Bezpieczeństwa Informacji, albo inną upoważnioną przez niego osobę.

2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym Administratora Bezpieczeństwa Informacji.

§ 5

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.
2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§ 6

Niezwłocznie po uzyskaniu informacji o naruszeniu danych osobowych należy podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych przez osoby niepowołane, poprzez:

1.) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,

2.) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,

3.) zmianę hasła na konto Administratora Bezpieczeństwa Informacji i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,

4.) zamknięcie i opieczętowanie urządzeń, w których przechowywane są dane osobowe w formie analogowej.

§ 7

Administrator Bezpieczeństwa Informacji, po uzyskaniu sygnału o naruszeniu danych osobowych, powinien w pierwszej kolejności:

1.) zapisać wszelkie informacje związane z danym zdarzeniem,

2.) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,

3.) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,

4.) wyniki postępowania zabezpieczającego oraz okoliczności naruszenia bezpieczeństwa danych osobowych należy ująć w raporcie i niezwłocznie przekazać Wójtowi Gminy Grębocice.

§ 8

1. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI lub upoważnionej przez niego osoby, należy:
   1.) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2.) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3.) zaniechać (o ile to możliwe) dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   4.) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   5.) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   6). zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   7). udokumentować wstępnie zaistniałe naruszenie,
   8). nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby upoważnionej.
2. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:
   1). zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu Gminy
   2). może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3). rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych.
   4). nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

§ 9

1. Po dokonaniu czynności zabezpieczenia danych osobowych i ustaleniu przyczyn naruszenia ochrony danych osobowych należy niezwłocznie przywrócić normalny stan działania.
2. Po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji i zasięgnięciu niezbędnych opinii proponuje postępowanie naprawcze, w którym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
3. Po przywróceniu prawidłowego stanu bazy danych osobowych, należy przeprowadzić szczegółową analizę, w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
4. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez kierownictwo Urzędu Gminy, Administratora Bezpieczeństwa Informacji oraz Pełnomocnika ds. Ochrony Informacji Niejawnych.
5. Analiza, o której mowa w ust. 3, powinna zawierać:
   - wszechstronną ocenę zaistniałego naruszenia,
   - wskazanie odpowiedzialnych,
   - wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.
6. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych, należy przeprowadzić dodatkowe szkolenie osób biorących udział przy przetwarzaniu danych osobowych.
7. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych, ABI niezwłocznie zarządza przeprowadzenie dodatkowego szkolenia dla osób biorących udział przy przetwarzaniu danych osobowych, dokumentację ze szkolenia dołącza do raportu określonego w §10.

§10

1. Po dokonaniu czynności przedstawionych powyżej ABI sporządza szczegółowy Raport, którego wzór stanowi załącznik do niniejszej Instrukcji, zawierający:
   - opis zdarzenia
   - przyczynę zaistnienia
   - skutki naruszenia ochrony danych osobowych
   - podjęte działania , zastosowane środki
   - analizę zdarzenia oraz wnioski dot. przedsięwzięć:

- organizacyjnych
- technicznych
- kadrowych

2. Raport ABI przedkłada niezwłocznie Wójtowi Gminy Grębocice, który wydaje pisemne zalecenia.
3. W terminie 90 dni Wójt wydaje polecenie dokonania kontroli wydanych zaleceń, określonych w ust.2, którą ABI przeprowadza niezwłocznie.
4. Nie wykonanie zaleceń, o których mowa w ust. 2 traktowane będzie jako ciężkie naruszenie dyscypliny w rozumieniu art. 52 ust.2 KP z uwagi na umyślny charakter działania sprawcy
5. Całość dokumentacji w zakresie naruszenia systemu ochrony danych osobowych przechowuje ABI.

§ 11

W zakresie nieuregulowanym niniejszą instrukcją, stosuje się odpowiednie przepisy Ustawy o ochronie danych osobowych oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Załącznik
do **Instrukcja postępowania**
w sytuacji naruszenia systemu
ochrony danych osobowych

Raport

z naruszenia bezpieczeństwa systemu informatycznego
w Urzędzie Gminy Grębocice

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

2. Osoba powiadamiająca o zaistniałym zdarzeniu:
.....
(Imię i nazwisko, stanowisko służbowe, nazwa użytkownika -jeśli występuje)

3. Lokalizacja zdarzenia:
.....
(np. nr pokoju, nazwa pomieszczenia)

4. Opis zdarzenia:
.....
(rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące)
.....
.....
.....
.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:
.....
.....
.....
.....
.....
.....
.....

6. Skutki naruszenia ochrony danych:
.....
.....
.....
.....
.....
.....
.....

7. Podjęte działania:

....
....
....
....
....
....
....
....
....

8. Postępowanie wyjaśniające:

....

(analiza zdarzenia oraz wnioski dot. przedsięwzięć organizacyjnych, technicznych, kadrowych

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

....

data, podpis Administratora Bezpieczeństwa Informacji

Załącznik **nr 3**
do **Polityki Bezpieczeństwa**

Urząd Gminy
w Grębocicach

Wykaz baz danych w systemach informatycznych w których przetwarzane są dane osobowe

L.p.	Nazwa bazy danych[1]	Wersja bazy danych	Forma bazy danych/System operacyjny serwera[2]	Sposób zabezpieczenia informatycz-nego[3]	Zawiera także dane osób spoza firmy (T/N)	Baza danych chroniona przez UPS (T/N)	Liczba miejsc przetwarzania i liczba porządkowa w załączniku nr 3
1.	USC		Program/ Windows XP	I	T	T	1
2.	EWID		Program/ Novell	I	T	T	1
3.	EGB III		Program/ Novell	I	T	T	1
4.	SIGID PODATKI		Program/ Novell	I	T	T	2

[1]nazwa zwyczajowa lub własna, np.: kadry, itp.
[2]np.: plik Excela/Windows 2000
[3]np.: (I) indywidualne hasło dostępu do bazy danych, (S) szyfrowanie bazy danych, (F) wydzielona fizycznie sieć

Dane aktualne na dzień:18./01/2007.

Sporządził:.....

Urząd Gminy
w Grębocicach

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów

L.p.	Nazwa bazy danych (1)	Imię i Nazwisko użytkownika	Nazwa identyfikatora	Rodzaj uprawnień(2)	Data zarejestrowania	Data wyrejestrowania	Lokalizacja (3)	Uwagi
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1.	SIGID PODATKI	Marianna Glapińska	Gm	Z, W	12.2004		Pok. 15	
2.	EWID	Mieczysława Janus	Danuta	Z, W	11.04.1999		Pok. 17	
3.	USC	Mieczysława Janus	Janus	Z, W	1.12.1998		Pok. 17	
4.	EGB III	Zuzanna Wiśniewska	adm	Z, W	01.1998		Pok. 3	
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								

1	2	3	4	5	6	7	8	9
14.								
15.								
16.								
17.								
18.								
19.								
20.								

[1]Nazwa bazy danych z załącznika nr 1
[2]Skróty stosowane do określenia uprawnień
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na ekranie
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych

Uwaga:
w przypadku praw ograniczonych do określonej części bazy danych, należy to ograniczenie podać w polu ***„Uwagi"***

[3]Należy podać liczbę porządkową zgodnie z załącznikiem nr 2

Dane aktualne na dzień:18./01/2007.

Sporządził:.....

Załącznik **nr 5**
do **Polityki Bezpieczeństwa**

Urząd Gminy
w Grębocicach

Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych

UWAGA: *do każdej lokalizacji należy dołączyć szkic sytuacyjny określający położenie stanowisk komputerowych w pomieszczeniu, z zaznaczeniem strefy ochronnej, do której nie mają dostępu osoby nieupoważnione, drzwi wejściowe, okna oraz zabezpieczenia fizyczne.*

L.p.	Nazwa bazy danych[1]	Lokalizacja (adres)	Nr pokoju /piętro	Funkcja lokalizacji [2]	Zabezpieczenie fizyczne [3]
1.	**USC**	Budynek Urzędu Gminy Głogowska 3, Grębocice	17/I	U, Z	-
2.	**EWID**	Budynek Urzędu Gminy Głogowska 3, Grębocice	17/I	U	-
3.	**EGB III**	Budynek Urzędu Gminy Głogowska 3, Grębocice	3/Parter	U	-
4.	**SIGID PODATKI**	Budynek Urzędu Gminy Głogowska 3, Grębocice	15/I	U	-

[1] nazwa bazy danych z załącznika nr 1
[2] (**S**) - serwer, (**K**) – miejsce przechowywania kopii bezpieczeństwa, (**Z**) – pomieszczenie w którym wykonywane są kopie bezpieczeństwa, (**U**) – pomieszczenie osób wprowadzających dane, (**A**) – pomieszczenie administratora bazy danych
[3] (**K**) – kraty w oknach, (**A**) – alarm, (**W**) – wzmocnione drzwi

Dane aktualne na dzień:18/01/2007.

Sporządził:.....

Załącznik **nr 6**
do **Polityki Bezpieczeństwa**

EWIDENCJA PRACOWNIKÓW

URZĘDU GMINY w GRĘBOCICACH

UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Komórka Organizacyjna	Imię i nazwisko	Stanowisko	Data wystawienia upoważnienia
1	2	3	4	5
1.	Kierownik Gminy	Roman Jabłoński	Wójt	Administrator danych
2.	Sekretarz Gminy	Edyta Jakubowska-Leśniak		
3.	Skarbnik Gminy	Barbara Jurcewicz		
4.	Referat Organizacyjny RO	Grażyna Chudzik		
		Henryk Drajkowski		
		Iwona Gidel		
		Danuta Burzyńska	Opiekun przewoz. szkol.	nie ma
		Stanisław Mierzwiak	Kierowca autobusu	nie ma
		Mariusz Bilski	Kierowca autobusu	nie ma
		Barbara Franczak	Sprzątaczka	nie ma
		Grażyna Szołtek	Robotnik gospodar.	nie ma
5.	Referat Finansowy RF	Aneta Hojdeczko	Kier. Referatu	
		Anna Sawicka		do końca 2007
		Marianna Glapińska		
		Magdalena Krakowiak		
		Monika Krysiak		czerwiec 2007
		Iwona Batycka		okresowe
		Emilia Płóciennik		
		Stanisława Popowicz		
6.	Referat Budownictwa i Gospodarki Komunalnej RB i GK	Urszula Nowak	po. Kier. Referatu	
		Małgorzata Litwin		
		Irena Marszał		
		Zygmunt Gaworski		

1	2	3	4	5
7.	**Referat Zagospodarowania Przestrzennego i Ochrony Środowiska RZP i GN**	**Joanna Idziak**	**Kierownik Referatu**	
		Teresa Pyszka		
		Zuzanna Wiśniewska		
8.	**Urząd Stanu Cywilnego USC**	**Mieczysława Janus**		
9.	**Stan. ds. Wojskowych, Zarządz. Kryzys. i OC GCR Obsł. Biura Rady i Promocji**	**Daniel Czajkowski**		

Aktualizacja: 05.01.2007 r.

---------- stażyści
---------- zatrudnieni czasowo
---------- bez upoważnień

Lista stażystów na 05.01.2007 r.

L.p.	Imię Nazwisko	Komórka organizacyjna	Data wydania upoważnienia
1.	Anna Głowacka	RB i GK	
2.	Barbara Maćkowiak	RO	
3.	Kataryna Lerke	RZP i GN	
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Załącznik **nr 7**
do **Polityki Bezpieczeństwa**

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

□*□ — zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285),

□*□— zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

□*□ — zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr .....

.....
(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:
.....

do Rejestru Zbiorów Danych Osobowych.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych):

.....
.....
.....
(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel Wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:

.....
.....
.....
(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:

□*□ — administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),

□*□ — administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

W przypadku powierzenia przetwarzania danych innemu podmiotowi podaj nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:

.....

.....

.....

.....

.....

.....

□ *□ *cd. w załączniku nr.....*

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

□*□ — zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,

□* □ — przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa —

.....

.....

.....

.....

□ * □ *cd. w załączniku nr.....*

□*□ — przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

□*□ — przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego — jeśli TAK, to opisz te zadania:

.....

.....

.....

.....

□*□ *cd. w załączniku nr.....*

□*□ — przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

5. Cel przetwarzania danych w zbiorze:

.....
.....
.....
.....

□*□ *cd. w załączniku nr*.....

6. Opis kategorii osób, których dane dotyczą:

.....
.....
.....

7. Zakres przetwarzanych w zbiorze danych o osobach:

□*□ — nazwiska i imiona,
□*□ — imiona rodziców,
□*□ — data urodzenia,
□*□ — miejsce urodzenia,
□*□ — adres zamieszkania lub pobytu,
□*□ — numer ewidencyjny PESEL,
□ * — Numer Identyfikacji Podatkowej,
□ * □— miejsce pracy,
□ * □— zawód,
□ * — wykształcenie,
□ *□ — seria i numer dowodu osobistego,
□* □ — numer telefonu.

8. Inne dane osobowe, oprócz wymienionych w pkt. 7, przetwarzane w zbiorze — *podaj jakie:*

.....
.....
.....
.....

□ *□ *cd. w załączniku nr*.....

9. Dane przetwarzane w zbiorze:

a) ujawniają bezpośrednio lub w kontekście:

□*□ — pochodzenie rasowe,
□*□ — pochodzenie etniczne,
□*□— poglądy polityczne,
□*□— przekonania religijne,
□*□— przekonania filozoficzne,
□*□— przynależność wyznaniową,
□ * — przynależność partyjną,
□* — przynależność związkową,
□*□— stan zdrowia,
□*□— kod genetyczny,
□*□ — nałogi,
□*□ — życie seksualne,

b) dotyczą:

□*□ — skazań,
□*□ —mandatów karnych,
□* □ — orzeczeń o ukaraniu,
□* □ — innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść od razu do pkt 11.

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:

□*□ — osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,
□* □ — przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych — *jeśli TAK, to podaj odniesienie do przepisu tej ustawy:*

.....
.....
.....
.....
.....

□*□ *cd. w załączniku nr*.....

□* □ — przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

□ *□ — przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych — *jeśli TAK, to podaj jakich:*

.....
.....

.....
.....

□*□*cd. w załączniku nr*.....

□ *□ — przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

□*□ — przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących
się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

□*□ — przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

□*□ — przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez
osobę, której dane dotyczą,

□*□ — przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,

□*□ — przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

11. Sposób zbierania danych do zbioru:

□ *□ — wyłącznie od osób, których dotyczą,
□ *□ — głównie od osób, których dotyczą,
□ *□ — wyłącznie z innych źródeł,
□ *□ — głównie z innych źródeł,
□*□ — głównie metodą teletransmisji,
□ *□ — również metodą teletransmisji.

12. Sposób udostępniania danych ze zbioru:

□ *□ — dane będą udostępniane wyłącznie podmiotom upoważnionym na podstawie przepisów prawa,

□*□ — dane będą udostępniane innym podmiotom,

□* □ — dane będą udostępniane również drogą teletransmisji.

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane — *podaj nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu dane mogą być przekazywane:*

.....
.....
.....
.....

□ *□ *cd. w załączniku nr*.....

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego — *podaj nazwę państwa:*

.....
.....
.....
.....

Część E. Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36—39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(w poniższych odpowiedziach proszę nie ujawniać szczegółów zastosowanych rozwiązań)

15. Zbiór danych osobowych będzie przetwarzany:

□□ — centralnie □□ — w architekturze rozproszonej

16. Przedsięwzięcia zastosowane w zakresie:

a) środków ochrony fizycznej danych:

.....
.....
.....
.....

b) środków sprzętowych, informatycznych i telekomunikacyjnych (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

.....
.....
.....
.....

c) środków ochrony w ramach oprogramowania urządzeń teletransmisji (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

.....
.....
.....
.....

d) środków ochrony w ramach oprogramowania systemów (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

.....
.....
.....
.....

e) środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

.....
.....
.....
.....

f) środków ochrony w ramach systemu użytkowego (nazwy zwyczajowo przyjęte albo symbole norm lub standardów technicznych):

.....
.....
.....
.....

g) środków organizacyjnych:

.....
.....
.....
.....

Część F. Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)

17. Zastosowano środki bezpieczeństwa na poziomie:
    □*□ — podstawowym,
    □ *□ — podwyższonym,
    □*□ — wysokim.

.....
(data, podpis i pieczęć wnioskodawcy)

---

* Jeżeli TAK, to zakreśl □ kwadrat literą „X".

Załącznik **nr 8**
do **Polityki Bezpieczeństwa**

Opis struktury zbiorów danych

1. Aplikacja[1)]: SIGID Podatki

Producent: **Zakład Systemów Informatycznych SIGID Sp. z o.o.**

Wykaz osób posiadających dostęp do aplikacji przy wykorzystaniu loginu i hasła.

L.p.	Imię i Nazwisko	Uprawnienia[2)]	Identyfikator
1.	**Marianna Glapińska**	A	Gm
2.			

[1)] np. - Rejestr Spraw Dzieci Powiatowego Zespołu do Spraw Orzekania o Niepełnosprawności, itp.
[2)] np. **A** - administrator; **Z** - zapis; **O** - odczyt;

2. Aplikacja[1)]: EWID

Producent: **KPG - Spółka z o.o. Biuro Informatyki**

Wykaz osób posiadających dostęp do aplikacji przy wykorzystaniu loginu i hasła.

L.p.	Imię i Nazwisko	Uprawnienia[2)]	Identyfikator
1.	**Mieczysława Janus**	A	**Danuta**
2.			

[1)] np. - Rejestr Spraw Dzieci Powiatowego Zespołu do Spraw Orzekania o Niepełnosprawności, itp.
[2)] np. **A** - administrator; **Z** - zapis; **O** - odczyt;

3. Aplikacja[1)]: USC

Producent: **TenSoft Sp. z o.o**

Wykaz osób posiadających dostęp do aplikacji przy wykorzystaniu loginu i hasła.

L.p.	Imię i Nazwisko	Uprawnienia[2)]	Identyfikator
1.	**Mieczysława Janus**	A	**Janus**
2.			

[1)] np. - Rejestr Spraw Dzieci Powiatowego Zespołu do Spraw Orzekania o Niepełnosprawności, itp.
[2)] np. **A** - administrator; **Z** - zapis; **O** - odczyt;

4. Aplikacja[1)]: EGB III

Producent: **Komputerowa Asocjacja Informacyjna BOGART sp. z o.o.**

Wykaz osób posiadających dostęp do aplikacji przy wykorzystaniu loginu i hasła.

L.p.	Imię i Nazwisko	Uprawnienia[2)]	Identyfikator
1.	**Zuzanna Wiśniewska**	A	**adm**
2.			

[1)] np. - Rejestr Spraw Dzieci Powiatowego Zespołu do Spraw Orzekania o Niepełnosprawności, itp.
[2)] np. **A** - administrator; **Z** - zapis; **O** - odczyt;

Załącznik **nr 9**
do **Polityki Bezpieczeństwa**

Sposób przepływu danych pomiędzy poszczególnymi systemami

Nazwa programu do przetwarzania danych[1)]	Sposób przepływu danych pomiędzy systemami
USC	Wszystkie programy w ramach jednego systemu
SIGID Podatki	
EGB III	
EWID	

[1)] **np. - RADIX Kasa; - RADIX Kadry – Płace; - BudżetPro; - itp.**

Załącznik **nr 10**
do **Polityki Bezpieczeństwa**

Określenie wykorzystanych środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

I. Wykorzystane środki bezpieczeństwa na poziomie podstawowym:

1. W systemie informatycznym służącym do przetwarzania danych osobowych w n/wym. programach:
   1) USC
   2) SIGID Podatki
   3) EGBIII
   4) EWID

   wykorzystano następujące mechanizmy kontroli dostępu do tych danych:
   a) dla każdego użytkownika odrębny identyfikator;
   b) dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

2. System informatyczny służący do przetwarzania danych osobowych zabezpieczono, w szczególności przed:
   1.) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego poprzez:
      a.) logowanie się do systemu operacyjnego przy wykorzystaniu hasła
      b.) logowanie do serwera w celu dostępu do baz danych poprzez login i hasło
   2.) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
      a.) każda ze stacji roboczych jest zasilana z urządzenia podtrzymującego napięcie zasilania na czas umożliwiający zapis danych i wyłączenie stacji roboczej.

3. System informatyczny służący do przetwarzania danych osobowych zabezpieczono w szczególności przed:
   a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego poprzez:
      • wykorzystanie Firewall'a sprzętowego Router Pentagram

- wykorzystanie programu antywirusowego NOD 32

b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez:
   - zabezpieczenie każdej stacji roboczej oraz serwera poprzez wykorzystanie urządzenia podtrzymującego napięcie zasilania na czas umożliwiający zapis danych i wyłączenie stacji roboczej lub serwera

c) przydzieleniem innej osobie identyfikatora użytkownika, który utracił uprawnienia do przetwarzania danych.

d) w przypadku wykorzystania hasła uwierzytelniania użytkowników, zmienia się je nie rzadziej niż co 30 dni, minimalna długość hasła to co najmniej 8 znaków.

e) dane osobowe przetwarzane w systemie informatycznym zabezpieczono przez wykonanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych

f) kopie zapasowe:
   - przechowywanie w pomieszczeniu serwerowni w metalowej szafie z zamkiem oraz w archiwum
   - kopie usuwane są niezwłocznie po ustaniu ich użyteczności
   - wytwarza się kopię zewnętrzna przechowywaną w Urzędzie Gminy w Grębocicach

4. Komputery przenośne wykorzystywane do przetwarzania danych osobowych zabezpieczono w następujący sposób:
   a.) wprowadzenie hasła na BIOS
   b.) uruchomienie opcji w BIOS-ie „BOOT C: only"
   c.) wprowadzenie hasła przy logowaniu do systemu operacyjnego
   d.) wprowadzenie szyfrowania folderów, w których przechowywane są dane osobowe
   e.) jeśli pozwalały na to warunki techniczne wprowadzono hasło w biosie dysku twardego

5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji – pozbawiono wcześniej zapisanych danych poprzez wyzerowanie przy wykorzystaniu specjalistycznego oprogramowania, w przypadku kiedy nie było to możliwe dokonano fizycznego uszkodzenia talerza dysku twardego
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawiono wcześniej zapisanych danych poprzez wyzerowanie powierzchni dyskowej przy wykorzystaniu specjalistycznego oprogramowania

c) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiającym ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

II. Wykorzystane środki bezpieczeństwa na poziomie wysokim:

1. System informatyczny służący do przetwarzania danych osobowych chroni przed zagrożeniami pochodzącymi z sieci publicznej poprzez:

a) kontrolę przepływu informacji pomiędzy systemami informatycznymi administratora danych a siecią publiczną przy wykorzystaniu Firewall'a sprzętowego Router Pentagram

b) kontrolę działań inicjowanych z sieci publicznej i sytemu informatycznego administratora danych poprzez kontrolę stacji roboczych poprzez program antywirusowego NOD 32

Na wszystkich stacjach roboczych należy wprowadzić środki bezpieczeństwa na poziomie wysokim, ze względu na dostęp do sieci publicznej.

PROCEDURY AWARYJNE

Dla zachowania bezpieczeństwa przetwarzanych danych w Urzędzie Gminy Grębocice należy przestrzegać zasad określonego postępowania w sytuacjach zwanymi sytuacjami awaryjnymi.

1). W przypadku naruszenia danych osobowych

Wszelkie zauważone przez użytkowników zjawiska mogące naruszyć bezpieczeństwo stacji komputerowej, osób, sprzętu, oprogramowania, dokumentów lub bezpieczeństwa fizycznego muszą być niezwłocznie zgłoszone do Administratora Bezpieczeństwa Informacji, Administratora Sieci – informatyka, Zarządzającego oprogramowaniem lub bezpośredniego przełożonego. Osoby te mają obowiązek określenia skali naruszenia bezpieczeństwa. Postępowanie jest określone w **Instrukcji postępowania w sytuacji naruszenia systemu ochrony danych osobowych** stanowiącej załącznik nr 2 do Polityki Bezpieczeństwa Urzędu Gminy Grębocice.

2). W przypadku zaniku zasilania

W przypadku braku oddzielnej (awaryjnej) linii zasilania energetycznego, która zasilałaby w energię elektryczną obiekty Urzędu Gminy Grębocice w przypadku braku napięcia w linii głównej, każde stanowisko komputerowe jest zabezpieczone urządzeniem podtrzymującym zasilanie elektryczne (zasilacz awaryjny UPS). Urządzenie to jest w stanie utrzymać pracę przez okres do 30 minut.

Po uzyskaniu informacji o wystąpieniu braku zasilania, pracownik przystępuje do bezpiecznego zakończenie pracy na stanowisku komputerowym zgodnie do zaleceń określonych w **Procedurach rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu** stanowiących załącznik nr 4 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3). W sytuacji wystąpienia zagrożenia terrorystycznego

Zagrożeniem terrorystycznym może być:

- znalezienie podejrzanej paczki (przedmiotu)
- otrzymanie podejrzanej przesyłki
- otrzymanie telefonu o podłożonym ładunku wybuchowym
- itp.

W takiej sytuacji **każdy pracownik jest zobowiązany powiadomić natychmiast swojego bezpośredniego przełożonego.**

Stosownie do stanowiska pracy, miejsca pracy oraz zakresu obowiązków służbowych, pracownicy Urzędu Gminy Grębocice powinni codziennie przed przystąpieniem do wykonywania czynności służbowych dokonać kontroli pomieszczeń służbowych pod kątem ukrycia podejrzanej paczki lub jakiegokolwiek podejrzanego przedmiotu. Wykonując te czynności należy szczególną uwagę zwrócić na kosze na śmieci, pomieszczenia ogólnodostępne jak np. toalety, gdyż do tych miejsc i przedmiotów w sposób niekontrolowany mają dostęp różne osoby spoza grona zatrudnionych pracowników.

W przypadku znalezienia podejrzanego przedmiotu znajdującego się w nietypowym miejscu w budynkach Urzędu, Kierownik komórki organizacyjnej niezwłocznie powiadamia o fakcie Wójta lub Sekretarza Gminy podejmując jednocześnie czynności zabezpieczające miejsce znalezienia, uniemożliwiając do niego dostęp innym osobom. Informację taką należy niezwłocznie przekazać również do Dyżurnego Policji.

W sytuacji takiej nie należy:

- ulegać panice
- dotykać i przemieszczać przedmiotu

Po przybyciu Policji, kierownictwa akcji przekazywane jest policjantowi, który od tego czasu jest dowódcą prowadzonej akcji. Pracownicy Urzędu Gminy ściśle wykonują polecenie wydawane przez kierującego akcją.

W przypadku otrzymania lub znalezienia budzącej podejrzenia przesyłki w żadnym przypadku nie należy jej otwierać.

Jeśli przesyłka została już otwarta i zawiera jakąkolwiek podejrzaną substancję w różnej postaci (płynnej, proszkowej) należy:

- nie ulegać panice,
- unikać bezpośredniego kontaktu z innymi osobami,
- nie dotykać lub przemieszczać przesyłki,
- nie wąchać zawartości przesyłki,
- pozamykać okna i drzwi w pomieszczeniu celem wstrzymania ruchu powietrza.

Powiadomiony o powyższym fakcie Kierownik komórki organizacyjnej podejmuje działania zabezpieczające miejsce informując jednocześnie Wójta lub w razie jego nieobecności Sekretarza Gminy. O powyższej sytuacji należy natychmiast powiadomić Policję, Straż Pożarną, Pogotowie Ratunkowe (placówkę służby zdrowia). Po przybyciu na miejsce służb

specjalistycznych kierownictwo akcji przekazane jest funkcjonariuszowi Straży Pożarnej lub Policji.

W przypadku otrzymania przez pracownika telefonicznej informacji o podłożonej na terenie obiektu Urzędu Gminy paczce z zawartością materiałów wybuchowych, substancji biologicznych lub chemicznych należy:

- nie ulegać panice,
- rozmowę prowadzić spokojnie i uprzejmie,
- udając trudności ze zrozumieniem osoby telefonującej, jak najdłużej przeciągać rozmowę, celem uzyskania jak najwięcej informacji o odgłosach dochodzących z miejsca dzwoniącego
- starać się uświadomić dzwoniącemu czy wziął pod uwagę możliwość spowodowania w wyniku zamachu, śmierci lub choroby wielu niewinnych osób, w tym i dzieci,
- dążyć do uzyskania jak najwięcej informacji o dzwoniącym i jego motywie działania,
- starać się wciągnąć dzwoniącego w rozmowę, która umożliwi wykonanie następnych czynności
- prowadzić rozmowę z osobą informującą odpowiadając na pytania przy pomocy **„Formularza prowadzonej rozmowy z osobą informującą"** stanowiącym załącznik do niniejszego dokumentu.

Powiadomiony o powyższym fakcie Kierownik komórki organizacyjnej informuje Wójta a w razie jego nieobecności Sekretarza Gminy. O powyższej sytuacji należy natychmiast powiadomić Policję, Straż Pożarną, Pogotowie Ratunkowe.

4). W sytuacjach wystąpienia klęsk żywiołowych (pożar, powódź)

W przypadku wystąpienia klęski żywiołowej (pożaru, powodzi, itp.) należy zastosować się do aktualnie obowiązujących instrukcji przeciwpożarowych i ewakuacyjnych Urzędu zawartych w Instrukcji Bezpieczeństwa Pożarowego Urzędu Gminy Grębocice oraz w Instrukcjach sporządzonych przez Zespoły Kryzysowe.

Podstawową czynnością użytkowników po zakończeniu pracy jest

zabezpieczenie nośników informacji i wyłączenie stacji komputerowej.

Załącznik **nr 1**
do **Procedury awaryjnej**

FORMULARZ PROWADZONEJ ROZMOWY
Z OSOBĄ INFORMUJĄCĄ O PODŁOŻONYM ŁADUNKU

Informacja dla prowadzącego rozmowę.

1. *Wypełniając formularz, należy właściwe informacje podkreślić lub wpisać w miejsca zaznaczone.*
2. *Formularz należy wypełniać w trakcie rozmowy lub bezpośrednio po jej zakończeniu.*

Kiedy ładunek zaczął lub zacznie działać?

Odp.: .....

.....

Gdzie znajduje się ładunek?

Odp.: .....

.....

Co zawiera ładunek?

Odp.: .....

.....

Jak wygląda?

Odp.: .....

.....

W którym konkretnym miejscu jest on umieszczony ?

Odp.: .....

.....

Dlaczego podłożył Pan (Pani) ładunek ?

Odp.: .....

.....

Skąd Pan (Pani) telefonuje ?

Odp.: .....

.....

Gdzie Pan (Pani) w tej chwili się znajduje ?

Odp.: .....

.....

Czy mogę Panu (Pani) w czymś pomóc ?

Odp.: .....

.....

Czy chce się Pan (Pani) z kimś skontaktować ?

Odp.: .....

.....

Czy jest Pan (Pani) konstruktorem ładunku ?

Odp.: .....

.....

Proszę podać swoje nazwisko i adres ?

Odp.: .....

.....

Inne pytania uzależnione od konkretnej sytuacji, które nasuną się w trakcie prowadzonej rozmowy

Pytanie .....

Odp.: .....

.....

.....

Pytanie .....

Odp.: .....

.....

.....

Dane personalne osoby przyjmującej wymienioną informację telefoniczną: .....

.....

Czas przyjęcia informacji: .....

Cechy charakterystyczne prowadzonej rozmowy:

- opis głosu rozmówcy

z jaką znaną osobą utożsamiasz głos rozmówcy .....

.....

Głos należał do osoby będącej: kobietą, mężczyzną, dzieckiem*)

Głos należał do osoby w wieku: młodym, średnim, starszym*)

W jakim wieku w przybliżeniu mogła być osoba dzwoniąca ? .....

Akcent rozmówcy: cudzoziemski, miejscowy (gwara, sztucznie zmieniany) .....

.....

....

Ton głosu: niski, wysoki, głośny, cichy, szybki, wolny, ciepły, chrapliwy, jąkający się, zniekształcony, bełkotliwy, sepleniący, nosowy*), inny .....

.....

Charakterystyczna wymowa którejś z głosek .....

Inne cechy charakterystyczne głosu .....

.....

Tło akustyczne np. cisza, jakieś dźwięki

Dźwięki w tle (odgłosy dochodzące z miejsca przebywania rozmówcy) np. ulica, fabryka, biuro, dworzec autobusowy lub kolejowy, głosy ludzkie, winda,*)

głosy zwierząt (jakich) .....

muzyka (jakiego rodzaju) .....

Zachowanie się dzwoniącego: spokojne, wesołe, rozsądne, rozgniewane, desperackie, aroganckie, nieracjonalne*), inne .....

.....

.....

Wpisać dokładną treść rozmowy: .....

.....

.....

.....

Inne uwagi przyjmującego informację telefoniczną: .....

.....

.....

.....

Kogo powiadomiono o informacji .....

.....

.....

.....
data i podpis przyjmującego informację

*) zaznaczyć właściwą cechę

Załącznik nr 2
do Zarządzenia nr 12/2007
Wójta Gminy Grębocice z dnia 18 stycznia 2007r.

Instrukcja

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Grębocicach

Wstęp

Nowelizacja przepisów ochrony danych osobowych w 2004 roku spowodowała wprowadzenie nowych unormowań prawnych regulujących przedmiotowe zagadnienie w zakresie dokumentacji związanej z zarządzaniem systemem informatycznym.

Jednym z nowych unormowań prawnych wydanych na podstawie Ustawy jest Rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100 poz. 1024).

Zgodnie z treścią powyższego aktu prawnego, jednym z wymogów, jaki został wprowadzony jest opracowanie w formie pisemnej **Instrukcji zarządzaniem systemem informatycznym służącym do przetwarzania danych osobowych**, której wdrożenie do stosowania w Urzędzie jest obowiązkiem Administratora Danych.

§ 1

Niniejsza Instrukcja stanowi podstawę do określenia sposobu zarządzania systemem informatycznym przy pomocy, którego przetwarzane są dane osobowe w Urzędzie Gminy w Grębocicach oraz prowadzenia szkoleń pracowników w zakresie ochrony danych osobowych. Zawiera informacje o systemie informatycznym oraz procedury i zasady podjęte w Urzędzie dla zapewnienia poufności, integralności i bezpieczeństwa przetwarzanych danych osobowych, które muszą być przestrzegane przez osoby odpowiedzialne w Urzędzie Gminy Grębocice za ich realizację zgodnie z posiadanymi uprawnieniami i zakresem obowiązków.

§ 2

Ilekroć w Instrukcji jest mowa o:

- **zbiorze danych** - rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny wg określonych kryteriów niezależnie czy jest to zestaw scentralizowany, rozproszony, jednolity lub podzielony funkcjonalnie.
- **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
- **danych osobowych** - rozumie się przez to każdą informację dotyczącą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- **Administratorze Danych** - rozumie się przez to organ samorządu terytorialnego tj. Wójta Gminy Grębocice.
- **ABI** - należy przez to rozumieć Administratora Bezpieczeństwa Informacji, osobę wyznaczoną przez Wójta do wykonywania czynności nadzorczych w zakresie ochrony danych osobowych w Urzędzie Gminy.
- **Administratorze Sieci** - rozumie się przez to osobę upoważnioną do zarządzania siecią informatyczną,
- **użytkowniku** - rozumie się przez to osobę upoważnioną przez Administratora Danych do dostępu i przetwarzania danych osobowych,
- **systemie informatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych do przetwarzania danych w Urzędzie Gminy.
- **zabezpieczeniu systemu informatycznego** - należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

§ 3

1. Administrator Danych Urzędu Gminy Grębocice wprowadza Instrukcje i upoważnia Administratora Bezpieczeństwa Informacji do nadzorowania wdrożenia sposobu administrowania i zarządzania środkami informatycznymi wspomagającymi procesy przetwarzania informacji stanowiących dane osobowe w rozumieniu Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 roku Dz.U. nr 101 poz. 926 wraz z późn. zm.).
2. Administrator Bezpieczeństwa Informacji odpowiada za korygowanie niniejszej Instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych zachodzących w Urzędzie.

§ 4

Administrator Danych stwarza właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo systemów informatycznych w Urzędzie w szczególności:

1. w przypadku systemów informatycznych służących do przetwarzania danych w zakresie:
   1.) lokalizacji pomieszczeń, w których przetwarzane są dane osobowe
   2.) lokalizacji pomieszczeń, w których przechowywane są kopie awaryjne zbiorów danych osobowych
   3.) instalowania krat i systemów alarmowych adekwatnych do zagrożenia systemów informatycznych
   4.) zakupu niszczarek do dokumentów do pomieszczeń, w których generowane są wydruki zawierające dane osobowe
   5.) zakupu szaf metalowych do przechowywania kopii zapasowych danych osobowych z systemów informatycznych
2. zabezpiecza budynki oraz pomieszczenia w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych, a w szczególności:
   1.) wprowadza i nadzoruje bieżącą aktualizację listy osób upoważnionych do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe

2.) wprowadza ewidencję osób pobierających klucze do pomieszczeń w których przetwarzane są dane osobowe zawierającą m.in. czas pobierania i zdawania kluczy w budynku, w którym przetwarzane są dane osobowe w systemach informatycznych
3.) określają tryb pobytu osób sprzątających pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych uwzględniający specyfikę obiektu

§ 5

Administrator Bezpieczeństwa Informacji Urzędu Gminy w Grębocicach:
1.) czuwa nad wdrażaniem niniejszej instrukcji w systemach informatycznych Urzędu, w których przetwarzane są dane osobowe oraz dba o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych urzędu
2.) określa strategię zabezpieczania systemów informatycznych Urzędu
3.) sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych
4.) sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe
5.) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Urzędu
6.) określa potrzeby w zakresie zabezpieczenia systemów informatycznych w których przetwarzane są dane osobowe
7.) sprawuje osobisty nadzór lub za pośrednictwem pisemnie upoważnionej osoby, nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, w których przetwarzane są dane osobowe,
8.) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych
9.) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolę dostępu do danych
10.) zgłasza potrzeby w zakresie zmiany w konfiguracji sprzętu lub oprogramowania mające wpływ na bezpieczeństwo systemu komputerowego
11.) sprawuje nadzór nad systemem komunikacji w sieci komputerowej oraz nad przesyłaniem danych za pośrednictwem urządzeń teletransmisyjnych

12.) określa zasady i ewidencję wykonywania czynności serwisowych w systemach informatycznych w celu wyeliminowania:

a.) możliwości wykonania kopii danych osobowych przez osoby nieupoważnione,

b.) przemieszczania urządzeń komputerowych i ich części służących do przetwarzania danych osobowych poza obszar objęty ochroną

c.) podmiany elementów sprzętu komputerowego lub oprogramowania na inny, który zawiera cechy ukryte

§ 6

1. Administrator Sieci w porozumieniu z Administratorem Bezpieczeństwa Informacji opracowuje i na bieżąco uaktualnia procedury wymienione w § 3 niniejszej Instrukcji.
2. Administrator Sieci dla zapewnienia bezpieczeństwa systemów informatycznych Urzędu:

1.) dokonuje wyboru lub migracji do technologii minimalizującej zagrożenie uzyskania dostępu do sieci osobom nieupoważnionym

2.) zgłasza potrzebę zakupu oprogramowania umożliwiającego rejestrowanie identyfikatorów i czas logowania użytkowników sieci

3.) nadzoruje proces monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych

4.) zakupu pamięci masowych, streamerów oraz innych urządzeń i nośników umożliwiających wykonywanie kopii zapasowych danych osobowych w systemach informatycznych

5.) zgłasza potrzebę zakupu systemów operacyjnych, oprogramowania antywirusowego oraz systemów kryptograficznych podnoszących bezpieczeństwo danych osobowych, gwaran-tujących spełnienie wymogów określonych ustawą

6.) dokonuje właściwego prowadzenia i zabezpieczenia okablowania sieci komputerowej służącej do przetwarzania danych osobowych w systemach informatycznych w celu wyeliminowania zagrożeń

§ 7

1. Administrator Bezpieczeństwa Informacji publikuje zatwierdzony dokument a kierownicy komórek organizacyjnych Urzędu Gminy Grębocice są zobowiązani zapoznać swoich

podwładnych z niniejszą Instrukcją.

4. Osoby, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt podpisaniem oświadczenia wg wzoru, który jest załącznikiem nr 3 do Zarządzenia nr 12/2007 Wójta Gminy Grębocice z dnia 18 stycznia 2007r. wprowadzającego dokumentację przetwarzania danych osobowych.
5. Oświadczenia takie przechowywane są w aktach personalnych pracownika w Referacie Organizacyjnym.

§ 8

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy w Grębocicach określa:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazania osoby odpowiedzialnej za te czynności – zał. Nr 1;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem – zał. Nr 2;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu – zał. Nr 3
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania – zał. Nr 4;
5) sposób, miejsce i okres przechowywania – zał. Nr 5:
   a) elektronicznych nośników informacji zawierających dane osobowe,
   b) kopii zapasowych, o których mowa w pkt. 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt. III ppkt 1 załącznika do Rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku (Dz.U. nr 100 poz. 1024) – zał. Nr 6;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 – zał. Nr 7;
8) procedury dokonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych – zał. Nr 8.

Załącznik
do **Instrukcji korzystania**
z systemu teleinformatycznego

Procedury korzystania z systemu informatycznego

PROCEDURA NR 1

Rejestracja w systemie informatycznym nowego pracownika

1. Po przeszkoleniu w zakresie BHP i ochrony danych osobowych bezpośredni przełożony (kierownik komórki organizacyjnej) zgłasza pracownika do systemu informatycznego przez wypełnienie dokumentu „Karta zgłoszenia do systemu".
2. „Karta zgłoszenia do systemu" składa się z IV części – wzór poniżej
   a). cz. I- wypełnia bezpośredni przełożony pracownika
      - imię i nazwisko
      - stanowisko
      - od kiedy ma mieć dostęp do systemu
      - na którym komputerze ma pracować
      - rodzaj oprogramowania
      - kogo zastępuje
      - podpis osoby wnioskującej

   b). cz. II - potwierdzenie o odbytym szkoleniu w zakresie ochrony danych osobowych i bezpieczeństwa systemu informatycznego - podpis osoby przeprowadzającej szkolenie

   c). cz. III - wypełnia Administrator Sieci
      - nadanie loginu i hasła,
      - przydzielenie poczty internetowej i intranetowej,
      - data nadania,
      - podpis

   d). cz. IV - potwierdzenie użytkownika o zapoznaniu się z instrukcją i prawidłowością

działania przydzielonej aplikacji.

3. Administrator Sieci przeprowadza czynności:
   - założenia konta,
   - ustalenia hasła startowego,
   - przygotowaniu komputera zgodnie z wytycznymi zawartymi w cz. I „Karty zgłoszenia do systemu"
4. Po zapoznaniu się z „Instrukcją korzystania z systemu teleinformatycznego" sprawdzeniu poprawności działania nadanych haseł, użytkownik w obecności administratora systemu podpisuje na „Karcie zgłoszenia do systemu" odbiór loginu i hasła (imię nazwisko, data). Administrator Sieci Urzędu Gminy narzuca zmianę hasła.
5. „Karta zgłoszenia do systemu" przechowywana jest w Serwerowni w wydzielonym segregatorze.

KARTA ZGŁOSZENIA DO SYSTEMU

Nr karty:.....*(Administrator Sieci)*

Część I

..... Grębocice, dn. .....

Referat

Proszę o nadanie uprawnień do systemu*)

Pani/ Panu*) .....

imię i nazwisko

....

stanowisko *numer pokoju*

W okresie od ..... do .....

Rodzaj aplikacji:

Standard:

- ✓ *Excel*
- ✓ *Konto poczty wewnętrznej*
- ✓ *Word*
- ✓ *7zip(program do archiwizacji)*
- ✓ *Acrobat Reader*
- ✓ *PowerPoint Viewer (przeglądarka prezentacji)*
- ✓ *Program antywirusowy*
- ✓ *Konto do wewnętrznego serwisu intranetowego*

Nie standardowe:

- ☐ *konto poczty zewnętrznej*
- ☐ *dostęp do Internetu*
- ☐ *LEX- System Informacji Prawnej*
- ☐ *PowerPoint (aplikacja do tworzenia prezentacji)*
- ☐ *Access*

Inne: .....

.....

data i podpis
bezpośredniego przełożonego

Część II

Potwierdzam odbycie szkolenia w zakresie ochrony danych osobowych i tajemnicy

……
data i podpis ABI

Część III

konto: .....

hasło (startowe): .....

Nazwa konta poczty wew: ....

Nazwa konta poczty zew: .....

Nazwa konta intranetowego: .....

Inne: .....

Wyposażenie – zgodnie z metryką komputera

Inne:.....

……
data i podpis Administratora Sieci

Cześć IV

Zapoznałam/em[*)] *się z „ Instrukcją korzystania z systemu teleinformatycznego"..*

……
data i podpis

[*)] - niepotrzebne skreślić

PROCEDURA NR 2

Usunięcie, blokada lub zmiana hasła użytkownika w systemie teleinformatycznym

- **Usunięcie** z systemu - oznacza trwałe odebranie uprawnień użytkownika do systemu teleinformatycznego (rozwiązanie umowy o pracę, staż, praktykę)
- **Blokada** w systemie - oznacza czasowe odebrania wszelkich uprawnień do systemu teleinformatycznego (urlop, choroba, inne)
- **Odblokowanie** w systemie - oznacza przywrócenie uprawnień
- **Zmiana hasła** – oznacza nadanie nowego hasła użytkownikowi związku z nieprawidłowym wprowadzeniem do systemu (dwa razy), zablokowaniem dłuższym niż zdefiniowana w systemie ważność hasła.

1. Pracownik wypełnia cz. I „Karty ….".
2. Bezpośredni przełożony użytkownika wypełnia cz. II
3. Administrator Sieci, który zgodnie z wytycznymi w części I dokumentu dokonuje zmiany w systemie. Po sprawdzeniu poprawności wykonania blokady/usunięcia oboje podpisują się na dokumencie. W przypadku blokady hasła, Administrator Sieci sprawdza parametry aktywności hasła, ustala nowe hasło tzw. „startowe", o którym powiadamia zainteresowanego.
4. „Karty blokady/usunięcia z systemu" archiwizowane są w serwerowni w wydzielonym segregatorze

KARTA USUNIĘCIA/BLOKADY W SYSTEMIE

Nr karty:.....(*nadaje Administrator Sieci)*

Część I

.....
Referat

Grębocice, dn. .....

Proszę o zablokowanie/odblokowanie/zmiana hasła /usunięcie w systemie[*)]

Pani/Pana[*)] .....

z powodu.....

od .....

do .....(dotyczy tylko zablokowania)

.....
data i podpis
użytkownika

Część II

Zatwierdzam zmiany zablokowania/odblokowania/zmiana hasła/usunięcia[*)] użytkownika z sytemu

.....
data i podpis
bezpośredniego przełożonego.

Cześć III

Zablokowanie/odblokowanie/zmiana hasła/usunięcie[*)] wykonano

Hasło startowe: .....

.....
data i podpis
Administratora Sieci

*)] - niepotrzebne skreślić

PROCEDURA NR 3

Modyfikacja uprawnień w systemie

Dotyczy zmiany istniejących uprawnień w związku:

- ze zmianą oprogramowania
- z przekazaniem zasobów po osobie zwalnianej lub przechodzącej na inne stanowisko
- z przejęciem zasobów okresowo na czas nieobecności pracownika (urlop, choroba, delegacja)

Zmiany opisane w procedurze nr 3 dotyczą tylko jednej komórki organizacyjnej.

W pozostałych przypadkach stosujemy procedury nr 1 i 2

- Pracownik wypełnia „ Kartę modyfikacji w systemie" - część I
- Administrator Bezpieczeństwa Informacji zatwierdza zmiany, jakie mają być wykonane w systemie - część II

  oraz dokonuje instalacji. Po sprawdzeniu poprawności wykonania blokady/usunięcia podpisuje się na dokumencie - część III
- „Karty modyfikacji systemu" archiwizowane są w serwerowni w wyznaczonym segregatorze.

KARTA MODYFIKACJI W SYSTEMIE

Nr karty:.....*(Administrator Sieci)*

Część I

.....
Referat

Grębocice, dn. .....

Proszę o dodanie/usunięcie*) niżej zaznaczonych aplikacji niestandardowych

Pani/Panu*).....

:

☐ *konto poczty zewnętrznej*

☐ *dostęp do Internetu*

☐ *LEX- System Informacji Prawnej*

☐ *PowerPoint (aplikacja do tworzenia prezentacji)*

☐ *Access*

inne :.....

lub udostępnienia

☐ profilu stacji roboczej numer ..... przypisanej do osoby .....

☐ zasobów sieciowych osoby.....

Data obowiązywania: od.....

.....
data i podpis pracownika

Część II

Zatwierdzam zmiany użytkownika w systemie

.....
data i podpis
Administratora Bezpieczeństwa Informacji

Cześć III

Modyfikację wykonano

.....
data i podpis
Administratora Sieci

PROCEDURA NR 4

Sposób zgłaszania awarii działania sprzętu komputerowego

1. Zgłoszenia awarii przyjmowane są telefonicznie do Administratora Bezpieczeństwa Informacji, który następnie informuje Administratora Sieci .
2. Po otrzymaniu telefonicznego zgłoszenia o awarii Administrator Sieci udaje się do stanowiska komputerowego zgłaszającego pracownika, gdzie ustala przyczynę powstania awarii.
3. Po usunięciu awarii sprawdza poprawność działania komputera.

PROCEDURA NR 5

Dostęp użytkowników do systemu informatycznego poza godzinami urzędowania

Standardowo w systemie informatycznym zdefiniowany jest dostęp w godzinach:

Poniedziałek	7.30 - 15.30
Wtorek	8.00 - 16.00
Środa	7.30 - 15.30
Czwartek	8.00 - 16.00
Piątek	7.30 - 15.30

Każda praca poza określonym terminem wymaga zgody bezpośredniego przełożonego, który powiadamia Administratora Bezpieczeństwa Informacji.

1. Bezpośredni przełożony pracownika wypełnia załącznik do procedury nr 5 - cześć I.
2. Po podpisaniu dokumentu, „Karta zmian godzin dostępu do systemu" przekazywana jest do Administratora Sieci.
3. Administratora Sieci, wprowadza zmiany w systemie informatycznym.
4. „Karta zmian godzin dostępu do systemu" archiwizowana jest w Serwerowni w osobnym segregatorze.

KARTA ZMIANY GODZIN PRACY

Nr karty:.....*(nadaje Administratora Sieci)*

Część I

..... Grębocice, dn. .....

Referat

Proszę o udostępnienie systemu informatycznego

Pani/ Panu *).....

imię i nazwisko

....

stanowisko *numer pokoju* *nr telefonu*

W godzinach od..... do.....

W okresie od .....do.....

... ...

data i podpis

bezpośredniego przełożonego

Część II

Zmiana godzin pracy wykonana

... ...

data i podpis

Administratora Sieci.

Część III

Anulowanie zlecenia

*) - niepotrzebne skreślić

PROCEDURA NR 6

Przyjęcia do ewidencji nowego sprzętu IT

(komputery, drukarki, switche, skanery, serwery, itp.)

Każdy nowo zakupiony sprzęt komputerowy przed przekazaniem do eksploatacji należy zarejestrować w systemie ewidencji środków trwałych (albo ewidencji wyposażenia) oraz w systemie finansowym.

1. Przesyłka (albo w przypadku samodzielnego odbioru: sprzęt) przekazywana jest do Sekretarza Gminy, a faktura i list przewozowy znajduje się w Referacie Finansowym.
2. Faktura jest rejestrowana w Referacie Finansowym
3. Referat Finansowy nadaje numer inwentarzowy dla sprzętu.
4. Administrator Sieci nanosi numer inwentarzowy na zakupiony sprzęt.

PROCEDURA NR 7

Wyposażenie stanowiska pracy w sprzęt IT

1. Każde stanowisko pracy jest wyposażone w „Specyfikację stanowiska komputerowego" w celu określenia jednoznacznej odpowiedzialności pracownika za powierzony sprzęt, którą to odpowiedzialność, pracownik akceptuje własnoręcznym podpisem na „Specyfikacji stanowiska komputerowego".
2. Po skonfigurowaniu komputera i podłączeniu do sieci pracownik sprawdza poprawność logowania i zainstalowanego oprogramowania.
3. Administrator Sieci wypełnia część dokumentu dotyczącą sprzętu komputerowego oraz zainstalowanego oprogramowania.
4. Pracownik przejmujący, sprawdza wyszczególniony sprzęt, zgodność numerów inwentarzowych, numerów fabrycznych i podpisuje „Specyfikację stanowiska komputerowego".
5. „Specyfikacja stanowiska komputerowego" przechowywana jest w serwerowni.
6. Przy zmianie w wyposażeniu wystawia się nową „Specyfikację stanowiska komputerowego" wypełniając ją w całości. Na starej karcie odnotowuje się zdanie sprzętu.
7. Przy zwolnieniu pracownika lub przekazywania stanowiska innemu pracownikowi, Administrator Sieci odnotowuje zdanie sprzętu na odwrocie karty, podpisując zgodność zdawanego sprzętu.

SPECYFIKACJA STANOWISKA KOMPUTEROWEGO

Pokój: [...] **Referat: [...]**

Użytkownik stanowiska: [.....]

IP komputera: [10 . 0 . 0 .] **Nazwa komputera w LAN [...]**

Numery seryjne	
Komputera	**Monitora**

Specyfikacja sprzętowa:

Numer inwentarzowy:[/ / /]

L.p.	Ogólna charakterystyka sprzętu	
1.	**Komputer:**	
2.	**Monitor:**	
3.	**Napęd CD/DVD:**	
4.	**FDD:**	
5.	**Inne:**	

Oprogramowanie:

L.p.	Nazwa programu	Uwagi
1.		
2.		
3.		
4.		
5.		
6.		
7.		

....

sporządził (data i podpis)

UWAGA:

1) Samowolne instalowanie jakiegokolwiek oprogramowania na powierzonym stanowisku komputerowym, bez wiedzy informatyka jest niedopuszczalne* !
2) Zabrania się samodzielnych zmian konfiguracji oprogramowania zainstalowanego na stanowisku.
3) Zabrania się przechowywania na dysku twardym komputera prywatnych dokumentów** !
4) Zabrania się samodzielnych zmian konfiguracji sprzętowej komputerów*** !

Potwierdzam zgodność specyfikacji sprzętu i oprogramowania (na powierzonym mi stanowisku) ze stanem faktycznym oraz akceptuję powyższe uwagi.

.....

(data i podpis)

---

* Dotyczy także „ładnych wygaszaczy" ekranu oraz wszelkiego pseudo-darmowego oprogramowania z internetu.

** Dotyczy prywatnych zdjęć, muzyki (w dowolnej formie), filmów (!!!) oraz wersji instalacyjnych oprogramowania komputerowego. **Wszelkie prywatne dokumenty będą kasowane z dysku komputera!**

***Dotyczy zmian w konfiguracji sprzętowej oraz zamiany komponentów zestawu pomiędzy stanowiskami.

PROCEDURA NR 8

Procedura postępowania przy korzystaniu z Internetu oraz poczty elektronicznej

1. W przypadku korzystania z sieci publicznej przy wykorzystaniu przeglądarki użytkownikowi zabrania się przebywania na stronach o tematyce pornograficznej, faszystowskiej, odwiedzania nielegalnych stron z kodami aktywacyjnymi do programów lub programami łamiącymi zabezpieczenia programów przed nielegalnym kopiowaniem.
2. Zabrania się użytkownikowi z korzystania z jakichkolwiek komunikatorów internetowych.
3. W przypadku, kiedy użytkownik stwierdzi lub przypuszcza, że odwiedzana strona internetowa w jakikolwiek sposób zagraża lub wywołuje nieprawidłowe działanie systemu operacyjnego zainstalowanego na stacji roboczej, powinien bezzwłocznie powiadomić bezpośredniego przełożonego i Administratora Bezpieczeństwa Informacji, który następnie zawiadomi Administratora Sieci.
4. W przypadku, kiedy służby informatyczne nie mogą interweniować z przyczyn niezależnych, użytkownik w momencie wystąpienia zagrożenia winien zamknąć przeglądarkę Internetową lub odłączyć kabel (skrętka) od stacji roboczej.
5. Użytkownikowi zabrania się wykorzystywania poczty elektronicznej do prowadzenia prywatnej korespondencji.
6. Użytkownikowi zabrania się otwierania podejrzanych załączników z poczty elektronicznej bez konsultacji z Administratorem Sieci.
7. Użytkownikowi zabrania się wypełniania formularzy oraz otwierania wiadomości z banków przesyłanych przy wykorzystaniu poczty elektronicznej. Tego rodzaju wiadomości, przesyłane są przez osoby próbujące uzyskać informacje o koncie bankowym, numerze rachunku oraz karcie kredytowej. Informacje te umożliwiają defraudację środków finansowych zgromadzonych na rachunkach użytkowników.

PROCEDURA NR 9

logowanie użytkownika do systemu lub aplikacji

Dostęp do aplikacji przetwarzających dane osobowe lub do sytemu operacyjnego zainstalowanego na stacji roboczej użytkownika powinien opierać się na podaniu przez użytkownika przyznanego mu przez Administratora Sieci identyfikatora oraz hasła.

1. Użytkownik korzysta z hasła startowego nadanego przez Administratora Sieci.
2. Po uwierzytelnieniu się w systemie użytkownik dokonuje zmiany hasła, które jest mu jedynie znane.
3. Po skończonej pracy użytkownik zobowiązany jest do zamknięcia aplikacji w sposób. uniemożliwiający jej ponowne uruchomienie bez procedury logowania.
4. Użytkownik korzystający z hasła i identyfikatora zobowiązany jest do zachowania tajemnicy odnośnie wymienionych elementów i nie może udostępniać tych informacji innym osobom.
5. Użytkownik może logować się do aplikacji tylko i wyłącznie przy wykorzystaniu swojego identyfikatora i hasła.
6. Zabronione jest, aby użytkownik swój identyfikator i hasło przechowywał w miejscu, z którego może zaistnieć możliwość przeczytania przez inne osoby.

PROCEDURA NR 10

Procedura wykorzystywania kopii bezpieczeństwa lub kopii zewnętrznej

1. W przypadku konieczności wykorzystania kopii bezpieczeństwa należy z szafy metalowej umieszczonej w pomieszczeniu w serwerowni pobrać kopię z dnia poprzedniego celem wykorzystania do przywrócenia stanu plików z dnia poprzedzającego. Utracone dane z dnia zaistnienia konieczności wykorzystania kopii zapasowej należy wprowadzić na bieżąco.
2. W przypadku zniszczenia kopii zapasowej należy wykorzystać kopię zewnętrzną.

Załącznik nr 2
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIA OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.

1. Po wykonaniu czynności kadrowych przez pracownika Referatu Organizacyjnego Urzędu Gminy Grębocice, kierownik komórki organizacyjnej wypełnia dokument w postaci **„Karta zgłoszenia do systemu"**, w przypadku samodzielnych stanowisk wymieniony dokument wypełnia Administrator Bezpieczeństwa Informacji.
2. Dokument wymieniony w pkt. 1 wypełniony przez kierownika komórki organizacyjnej przekazywany jest do Administratora Bezpieczeństwa Informacji, który sprawdza treść pod względem formalnym i merytorycznym.
3. W przypadku wystąpienia uwag, ABI zwraca dokument do uzupełnienia, natomiast przy braku uwag rejestruje użytkownika w prowadzonej ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Urzędzie, o czym informuje kierownika komórki organizacyjnej oraz Administratora Sieci.
4. Wszyscy pracownicy Urzędu Gminy Grębocice przetwarzający dane w systemach informatycznych posiadają konto z ograniczeniami.
5. W Urzędzie Gminy Grębocice tylko Administrator Bezpieczeństwa Informacji **(admin)** posiada konto bez ograniczeń i uprawnienia wprowadzania zmian do systemu. W przypadku nieobecności Administratora Bezpieczeństwa Informacji zastępstwo pełni osoba wyznaczona przez Administratora Danych.
6. Administrator Bezpieczeństwa Informacji jest uprawniony (na wniosek kierownika komórki organizacyjnej) do modyfikowania uprawnień lub usuwania kont użytkowników z systemu.
7. Osobą odpowiedzialną w Urzędzie Gminy Grębocice za realizację procedur oraz rejestrowanie i wyrejestrowanie użytkownika w systemie jest Administrator Bezpieczeństwa Informacji.
8. Czynności wymienione w pkt. 4, 6, 7 Administrator Bezpieczeństwa Informacji zleca wykonanie Administratorowi Sieci.

Załącznik nr 3
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. W Urzędzie Gminy Grębocice obowiązuje forma pisemna przydzielania hasła użytkownikom.
2. Hasło musi być złożone, składające się z 8-miu znaków w postaci małych i wielkich liter oraz cyfr lub znaków specjalnych.
3. Hasła przedzielone użytkownikowi nie mogą być powtarzane, a użyte do hasła znaki posiadają zestaw mieszany.
4. Administrator Sieci w obecności Administratora Bezpieczeństwa Informacji nadaje nowemu pracownikowi login i hasło startowe umożliwiające pracę w systemie.
5. Użytkownik systemu w obecności ABI uwierzytelnia się w systemie, a następnie zmienia nadane mu przez Administratora Sieci hasło i rozpoczyna pracę w aplikacji.
6. Za przydział haseł jest odpowiedzialny Administrator Bezpieczeństwa Informacji.
7. W Urzędzie Gminy Grębocice jest zakaz przekazywania hasła przez osoby inne niż wymienione w pkt. 3 i za pośrednictwem niezabezpieczonej poczty elektronicznej.
8. Zmiany hasła może dokonywać tylko Administrator Bezpieczeństwa Informacji Urzędu Gminy Grębocice.
9. Hasło dostępu w formie pisemnej każdy użytkownik przekazuje w zaklejonej kopercie do dyspozycji Administratora Bezpieczeństwa Informacji.
10. Koperty z hasłami użytkowników przechowywane są przez Administratora Bezpieczeństwa Informacji w szafie metalowej bez możliwości dostępu osób nieupoważnionych.
11. Otwarcie koperty z hasłem przez Administratora Bezpieczeństwa Informacji może nastąpić w szczególnych sytuacjach wymagających dostania się do konta użytkownika w czasie jego nieobecności. Po przybyciu, użytkownik dokonuje zmiany hasła powtarzając czynność jak w pkt. 9.
12. Hasła zmieniane są samodzielnie przez pracownika nie rzadziej, niż co 30 dni, gdyż system nie wymusza dokonania takich zmian.

Załącznik nr 4
do Instrukcji zarządzania
systemem informatycznym
służącym do przetwarzania
danych osobowych

PROCEDURY
ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY
PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

I. Procedura rozpoczęcia pracy

1). Dokonać uruchomienia komputera, który jest podłączony do sieci lokalnej Urzędu Gminy Grębocice.
2). Dokonać zalogowania się do sieci przez podanie swojego identyfikatora, a następnie hasła dostępu do sieci.
3). Następnie uruchomić aplikację podając swój identyfikator i hasło dostępu do aplikacji.
4). Po uzyskaniu dostępu do aplikacji rozpocząć pracę.

II. Procedura zawieszenia pracy w systemie

1). Każdorazowe odejście od stanowiska komputerowego w czasie pracy musi być poprzedzone zamknięciem programu, w którym przetwarzane są dane, aby na ekranie monitora nie były wyświetlane dane osobowe.
2). Przy dłuższej nieobecności dokonać wylogowania się z systemu lub włączyć blokadę komputera.
3). W przypadku opuszczenia pokoju, w którym nie pozostaje pracownik, należy pomieszczenie zamknąć uniemożliwiając dostęp osobom nieuprawnionym.

III. Procedura zakończenia pracy

Przy zakończeniu pracy postępuje się w odwrotnej kolejności do rozpoczęcia pracy.

1). Dokonać zamknięcia aplikacji, w której wykonywana była praca przetwarzania danych
2). Dokonać zamknięcia systemu

3). Wyłączyć monitor oraz drukarkę

4). W przypadku wykorzystywania urządzenia podtrzymującego (UPS) – wyłączy urządzenie

1. Przedstawione czynności w zakresie rozpoczęcia, zawieszenia czy zakończenia pracy, każdy pracownik wykonuje osobiście i samoczynnie.
2. Dostęp do przetwarzanych danych w danym zbiorze ma tylko pracownik, który je przetwarza oraz wskazana osoba przez Administratora Bezpieczeństwa Informacji.
3. W przypadku zaistnienia sytuacji tymczasowego zaprzestania pracy poprzez opuszczenie stanowiska zastosowane jest zabezpieczenie w postaci wygaszacza ekranu.
4. Wyrejestrowanie użytkownika z systemu następuje automatycznie z chwilą wyłączenia komputera.
5. W przypadku wystąpienia sytuacji podejrzenia naruszenia bezpieczeństwa systemu objawiającej się brakiem możliwości zalogowania się użytkownika na jego konto, bądź w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe, każdy pracownik-użytkownik ma obowiązek zgłoszenia tego faktu Administratorowi Bezpieczeństwa Informacji, który sprawdza wszystkie okoliczności danej sytuacji.

Załącznik nr 5
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Kopie zapasowe w Urzędzie Gminy są wykonywane w cyklu codziennym i miesięcznym. W cyklu codziennym z utworzonego pliku na stanowisku komputerowym dane przesyłane są na serwer, a następnie w cyklu miesięcznym nagrywane są na płytę DVD. Kopie wykonywane są metodą całościową.
2. Kopie zapasowe wykonywane są na płytach CD i DVD przy pomocy programu **COBIAN BACKUP w.7**
3. Nadzór nad wykonywaniem kopii zapasowych ich weryfikacją i poprawnością sprawuje Administrator Bezpieczeństwa Informacji Urzędu Gminy Grębocice.
4. Likwidacja nośników zawierających kopie zapasowe danych dokonywana jest po ich wycofaniu na skutek utraty przydatności. W przypadku uszkodzenia nośnika CD lub DVD likwidacja następuje w niszczarce do płyt. Dyski zawierające dane osobowe, przeznaczone do likwidacji pozbawia się wcześniej zawartych danych, a gdy nie jest to możliwe poprzez uszkodzenie w sposób uniemożliwiający ich odczytanie.
5. Czynność wymieniona w pkt. 3 wykonywana jest przez osobę wskazaną przez Administratora Bezpieczeństwa Informacji zgodnie z wymogami zawartymi w pkt. VI ppkt.1 załącznika do Rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku (Dz.U. nr 100 poz. 1024).

Załącznik nr 6
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA:

a) elektronicznych nośników informacji zawierających dane osobowe,

1). Dane osobowe w postaci elektronicznej przetwarzane w Urzędzie Gminy Grębocice zapisywane na dyskach twardych, dyskach magnetooptycznych, bądź dyskietkach, nie są wynoszone poza teren budynku.

2). Wszelkiego rodzaju nośniki informacji (dyskietki, płyty CD, DVD, taśmy magnetyczne), na których zapisywane są dane osobowe przechowywane są w zamkniętej szafie metalowej w pokoju serwerowni. Cześć natomiast jest przechowywana w archiwum.

3). W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik przez spalenie lub rozdrobnienie uniemożliwiające jego nieuprawnione wykorzystania (patrz Procedura – zał. Nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych).

4). Dyski twarde z danymi osobowymi należy zniszczyć zgodnie z obowiązującymi w Urzędzie Gminy Grębocice przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi.

b) kopii zapasowych,

1). Kopie zapasowe zbiorów danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych dla zabezpieczenia przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem są przechowywane w szafach metalowych w pokoju serwerowni oraz w archiwum.

c) kopii awaryjnych,

1). Kopie awaryjne zbiorów danych osobowych zabezpieczone są tak samo jak kopie zapasowe. Po ustaniu użyteczności są bezzwłocznie usuwane.

Załącznik nr 7
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, O KTÓRYM MOWA W PKT III PPKT 1 ZAŁĄCZNIKA DO ROZPORZĄDZENIA

1. System informatyczny w Urzędzie Gminy Grębocice jest najbardziej narażony na ingerencję wirusów komputerowych ze strony WWW lub za pośrednictwem POCZTY do których może przedostać się szkodliwe oprogramowanie.
2. Dla zminimalizowania skutków zainstalowania się szkodliwego oprogramowania sieć Urzędu Gminy została zabezpieczona programem antywirusowym **Nod32**, Firewall sprzętowy **Planet**.
3. Prowadzona jest codzienna aktualizacja wirusów przez Administratora Sieci Urzędu Gminy.
4. W przypadku zidentyfikowania określonego typu zagrożenia użytkownik powiadamia telefonicznie Administratora Bezpieczeństwa Informacji.
5. Każdy użytkownik sieci komputerowej Urzędu Gminy został poinformowany o postępowaniu w przypadku sygnalizowania przez oprogramowanie zabezpieczające o wykryciu wirusa.

Załącznik nr 8
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

ZASADY I SPOSÓB ODNOTOWYWANIA W SYSTEMIE INFORMACJI O UDOSTĘPNIENIU DANYCH OSOBOWYCH

1. System nie zapewnia odnotowywanie informacji o udostępnieniu danych. Obowiązek ten spoczywa na użytkowniku systemu, który odnotowuje ten fakt w odpowiednio przeznaczonym polu w bazie danych.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   - osoby, której dane dotyczą,
   - osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie,
   - przedstawiciela, o którym mowa w art. 31 a Ustawy o ochronie danych osobowych,
   - podmiotu, któremu powierzono przetwarzania danych,
   - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3. Odnotowywane informacje obejmują:
   - Data przekazania danych,
   - Nazwę jednostki organizacyjnej lub imię i nazwisko osoby, której przekazano dane,
   - Zakres przekazanych danych,
4. Wypełnienie wspomnianego pola następuje z chwila przekazania danych osobowych.
5. Udostępnianie danych osobowych następuje wyłącznie na pisemną prośbę odbiorcy danych – w formie wniosku, o którym mowa w art. 29 Ustawy o ochronie danych osobowych.
6. Nadzór nad prawidłowym odnotowywaniem informacji o udostępnionych danych osobowych sprawuje Administrator Bezpieczeństwa Informacji.

Załącznik nr 9
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Konserwacja urządzeń tworzących system informatyczny Urzędu Gminy Grębocice jest wykonywana co pół roku, natomiast przeglądy wykonywane są codziennie.
2. W Urzędzie Gminy Grębocice uprawnionymi do przeprowadzania przeglądów i konserwacji jest pracownik Firmy „NSI" z Głogowa, z którą Urząd Gminy posiada zawartą umowę na wykonywanie usług z zakresu IT.
3. W przypadku zaistnienia potrzeby przekazania sprzętu komputerowego do naprawy przez specjalistów Firmy zewnętrznej są wykonywane kopie danych zawartych na dyskach, po czym następuje wymontowanie dysku z komputera.
4. Przegląd programów i narzędzi programowych (np. zmiana wersji oprogramowania serwera, zmiana wersji oprogramowania stanowiska komputerowego użytkownika, zmiana systemu operacyjnego serwera, wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, modyfikacji czy konserwacji systemu) jest dokonywany w zależności od wystąpienia takiej potrzeby.
5. W przypadku wystąpienia sytuacji, w której nie ma możliwości wymontowania dysku z urządzenia postępowanie jest prowadzone zgodnie z wymogiem określonym w punkcie VI ppkt. 3 załącznika do Rozporządzenia, który nakazuje, aby urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy, pozbawiać wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawiać je pod nadzorem osoby upoważnionej przez administratora danych.

Załącznik nr 10
do **Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

Instrukcja korzystania z systemu teleinformatycznego

§ 1

Użytkownikom stacji roboczych zabrania się:

1. Udostępniania hasła innym osobom oraz przechowywania go w formie pisemnej w łatwo dostępnym miejscu,
2. Instalowania oprogramowania,
3. Podłączania jakichkolwiek urządzeń peryferyjnych (np.: pen-drive, aparat cyfrowy, drukarka),
4. Konfigurowania kont pocztowych
5. Udostępniania danych służbowych osobom nieuprawnionym poprzez pocztę elektroniczną oraz inne nośniki danych (np.: dyskietka, CD),
6. Wykorzystywania służbowej poczty do celów prywatnych,

§ 2

Każdy użytkownik stacji roboczej zobowiązany jest do:

1. Okresowej zmiany hasła zgodnie z polityką haseł (min. długość hasła – 8 znaków, hasło powinno być unikatowe, złożone z małych i dużych znaków oraz cyfr lub znaków specjalnych).
2. Blokowania stacji przy każdorazowym opuszczeniu stanowiska pracy.
3. *N a t y c h m i a s t o w e g o* poinformowania Administratora Bezpieczeństwa Informacji o każdej nieprawidłowości mogącej mieć wpływ na naruszenie bezpieczeństwa systemu teleinformatycznego.

Załącznik nr 3
do Zarządzenia nr 12 /2007
Wójta Gminy Grębocice z dnia 18 stycznia 2007r..

.....
imię i nazwisko pracownika

OŚWIADCZENIE

Oświadczam, że zapoznałem się z treścią:

„Polityki Bezpieczeństwa" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Grębocice".

Zobowiązuję się do stosowania zasad zawartych w tym dokumencie.

Grębocice, dnia .....

.....
podpis pracownika