Załącznik Nr 1
do Zarządzenia Nr
Wójta Gminy Boleszkowice
z dnia 16 lutego 2011r.

POLITYKA BEZPIECZEŃSTWA I INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W URZĘDZIE GMINY BOLESZKOWICE

Boleszkowice, Luty 2011 r.

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemie informatycznym w lokalnej sieci komputerowej oraz zbiorów danych zapisanych w postaci dokumentacji papierowej w Urzędzie Gminy Boleszkowice.

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

Dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926),
2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Boleszkowice", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób zabezpieczenia systemów informatycznych postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z §3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18, poz. 162) oraz §3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   a) stwierdzono naruszenie zabezpieczeń systemu informatycznego,
   b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy Boleszkowice.

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym Urzędu.
4. Administratorem Danych jest Wójt Gminy Boleszkowice.
5. Administrator Danych swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej „Administratorem Bezpieczeństwa".
6. „Administrator Bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:
   a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   b) 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,
   c) niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   d) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

ROZDZIAŁ I

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

   a) 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,
   b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenie 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 systemu z jego wnętrza, nie uprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana itp.;
b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego,
c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,
d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony danych osobowych albo inne strzeżone elementy systemu zabezpieczeń,
j) 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.,
k) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
l) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
m) 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.).

3. 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.

ROZDZIAŁ II

SPOSÓB I ZAKRES UDOSTEPNIANIA DOKUMENTU

1. Z dokumentem powinny zostać zapoznane osoby upoważnione do przetwarzania danych osobowych w zbiorach danych, a w szczególności:
   a) pracownicy Urzędu Gminy Boleszkowice,
   b) obsługa informatyczna Urzędu,
   c) inne osoby, jeżeli z zakresu obowiązków tych osób wynika konieczność dostępu do zbioru danych osobowych.

2. Za rozpowszechnienie dokumentu i zapoznanie z dokumentem przez poszczególnych użytkowników odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

ROZDZIAŁ III

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem Danych Osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Gminy Boleszkowice, jest Wójt Gminy Boleszkowice,

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

3. Do zastosowanych środków technicznych należy:
   a) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   b) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt poprzednim,
   c) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji,

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
   a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   b) przeszkolenie osób, o których mowa w punkcie poprzednim, w zakresie bezpiecznej obsługi urządzeń i zakresie programów związanych z przetwarzaniem i ochroną danych osobowych,
   c) 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,

5. Niezależnie od niniejszych zasad opisanych w dokumencie "Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Boleszkowice" 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.

6. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz wykaz zbiorów danych osobowych wraz z programami zastosowanymi do przetwarzania tych danych zawiera Załącznik nr 1 do Polityki Bezpieczeństwa do niniejszego dokumentu.

7. Stosowane zabezpieczenia służące ochronie przed utratą danych w Urzędzie Gminy Boleszkowice zawiera Załącznik nr 2 do Polityki Bezpieczeństwa.

ROZDZIAŁ IV

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator Danych (Wójt) lub osoba przez niego wyznaczona, którą jest "Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa Informacji sporządza półroczne plany kontroli zatwierdzone przez Wójta 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, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia Administratorowi Danych (Wójtowi).

ROZDZIAŁ V

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik Urzędu Gminy , który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa.

2. W razie niemożności zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

a) 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,
b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
c) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
g) udokumentować wstępnie zaistniałe naruszenie,
h) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora danych,
nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport (zał. Nr 3), który powinien zawierać w szczególności:

wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
określenie czasu i miejsca naruszenia i powiadomienia,
określenie okoliczności towarzyszących i rodzaju naruszenia,
wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
wstępną ocenę przyczyn wystąpienia naruszenia,
ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

Raport, o którym mowa w pkt 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.

Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzanych danych.

6. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora Danych, Administratora Bezpieczeństwa, Pełnomocnika ds. Ochrony Informacji Niejawnych.
7. Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

ROZDZIAŁ VI

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   a) Administrator Danych,
   b) Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególną uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   b) kontrola ewidencji nośników magnetycznych,
   c) kontrola właściwej częstotliwości zmiany haseł.

ROZDZIAŁ VII

SZKOLENIA

1. Szkolenie podstawowe dotyczące bezpieczeństwa danych obejmuje wszystkich pracowników Urzędu Gminy.
2. Szkoleniem szczegółowym obejmuje się pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych.
3. Tematyka szkoleń obejmuje:
   a) Przepisy i instrukcje wewnętrzne dotyczące ochrony danych, archiwizacji zasobów i przechowywania nośników, niszczenie wydruków i zapisów na nośnikach magnetycznych i optycznych,
   b) Zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.

ROZDZIAŁ VIII

ARCHIWIZOWANIE DANYCH

1. Administrator systemu wykonuje cotygodniowe kopie zapasowe zapisane w programie, oraz kopie bezpieczeństwa nie rzadziej niż co 6 miesięcy.

2. Kopie zapasowe przechowywane są w miejscu pracy, zaś kopie bezpieczeństwa poza budynkiem Urzędu Gminy na nośnikach cyfrowych. .

3. Nośniki, na których zapisywane są kopie zapasowe oraz kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, aby nie można było odtworzyć ich zawartości. Płyty CD lub DVD niszczy się trwale w sposób mechaniczny.

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

5. Nośniki z kopiami awaryjnymi oraz kopiami bezpieczeństwa przechowywane są w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym oraz chronione przed skutkami klęsk żywiołowych w postaci pożaru lub powodzi.

ROZDZIAŁ IX

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki cyfrowe przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów odbywa się poprzez wymazywanie informacji oraz formatowanie nośnika.
2. Poprawność przygotowania nośnika cyfrowego jest sprawdzana przez Administratora Bezpieczeństwa.
3. Uszkodzone nośniki cyfrowe przed ich wyrzuceniem są fizycznie niszczone poprzez przecięcie, przełamanie, itp.
4. Po wykorzystaniu wydruki zawierające dane osobowe są niszczone w stopniu uniemożliwiającym ich odczytanie, w specjalnym urządzeniu np. w mechanicznej niszczarce do papieru.

ROZDZIAŁ X

PROCEDURY NADAWANIA I ZMIANY UPRAWNIEŃ DO PRZETWARZANIA DANYCH

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późno zm.),
   b) niniejszym dokumentem.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **Załącznik nr 4 do Polityki Bezpieczeństwa.**

3. Przetwarzanie danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych, którego wzór stanowi **Załącznik nr 5 do Polityki Bezpieczeństwa.**

4. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie wydanego upoważnienia przez Administratora Danych Osobowych.

5. Jedynie prawidłowo wypełniony wniosek o nadanie uprawnień w systemie oraz zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie.

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

7. Jeżeli hasło zostało ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji, to należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.

8. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

9. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

10. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

11. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

12. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do systemu operacyjnego oraz dostępu do aplikacji.

13. Odebranie uprawnień pracownikowi następuje na pisemny wniosek bezpośredniego przełożonego, któremu podlega pracownik z podaniem daty oraz przyczyny odebrania uprawnień.

14. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.

15. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować dostęp do systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

16. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

17. Rejestr, którego wzór stanowi **Załącznik nr 6 do Polityki Bezpieczeństwa** powinien zawierać:

a) imię i nazwisko użytkownika systemów informatycznych,
b) rodzaj uprawnienia,
c) datę nadania uprawnienia,
d) datę odebrania uprawnienia,
e) przyczynę odebrania uprawnienia,
f) podpis administratora bezpieczeństwa informacji.

18. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

ROZDZIAŁ XI

ZASADY POSŁUGIWANIA SIĘ HASŁAMI

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

2. Hasło użytkownika powinno być zmieniane co najmniej raz na 30 dni.

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po zablokowaniu użytkownika w systemie informatycznym nie powinien być przydzielany innej osobie.

4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

8. Przy wyborze hasła obowiązują następujące zasady:
   1) minimalna długość hasła - 8 znaków,
   2) zakazuje się stosować:
      a) haseł, które użytkownik stosował uprzednio w okresie trzech miesięcy,
      b) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
      c) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
      d) wyrazów słownikowych,
      e) przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", 123456",itp.
   3) należy stosować:
      a) hasła zawierające kombinacje liter i cyfr,
      b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala
      c) hasła, które można zapamiętać bez zapisywania,
      d) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

9. Zmiany hasła nie wolno zlecać innym osobom poza Administratorem Bezpieczeństwa

10. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

11. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
    a) Administrator Bezpieczeństwa Informacji,
    b) Administrator Danych Osobowych lub osoba przez niego wyznaczona.

ROZDZIAŁ XII

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.

3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.

4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych

programów, wykonać zamknięcie systemu.

5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem uruchomionego oprogramowania bazodanowego.

6. Przypadki stwierdzenia nieprawidłowości systemu należy zgłaszać do Administratora Systemu.

ROZDZIAŁ XIII

SPOSÓB I MIEJSCE PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ WYDRUKÓW

1. Po zakończeniu pracy przez użytkowników systemu, nośniki magnetyczne, flashowe czy optyczne są przechowywane w zamykanych szafach biurowych.

2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

3. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

4. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.

ROZDZIAŁ XIV

ŚRODKI OCHRONY SYSTEMU PRZED ZŁOŚLIWYM OPROGRAMOWANIEM, W TYM WIRUSAMI KOMPUTEROWYMI

l. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.

2. Każdy e-mail wpływający do urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.

3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.

4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.

5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.

6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach.

8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie inne nośniki danych, które mogły być użyte przed wykryciem wirusa.

ROZDZIAŁ XV

ZASADY UDOSTĘPNIANIA DANYCH ORAZ REJESTRACJI ZBIORÓW DANYCH OSOBOWYCH

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie na wniosek do Administratora Danych wg wzoru **Załącznik nr 7 do Polityki Bezpieczeństwa.**

2. Udostępnienie zbiorów danych może nastąpić po wyrażeniu zgody przez Administratora Danych oraz Administratora Bezpieczeństwa Informacji. Zgoda nie jest wymagana, jeśli udostępnienie danych wynika z zakresu zadań tej jednostki organizacyjnej Urzędu, w dyspozycji której znajdują się te dane.

3. Administrator Bezpieczeństwa Informacji może odmówić udostępnienia danych, jeżeli może to naruszyć bezpieczeństwo i ochronę danych zgromadzonych w Systemie Informatycznym Urzędu.

ROZDZIAŁ XVI

POŁĄCZENIE DO SIECI INTERNET

1. Połączenie lokalnej sieci komputerowej urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych oraz kompleksowego oprogramowania antywirusowego.

2. Do zabezpieczenia sieci należy stosować:
   a) Firewall,
   b) Systemy antywirusowe.

ROZDZIAŁ XVII

REGULAMIN UŻYTKOWANIA OPROGRAMOWANIA I SPRZĘTU KOMPUTEROWEGO W URZĘDZIE GMINY BOLESZKOWICE

1. Każdy komputer użytkowany w Urzędzie powinien mieć zainstalowany program antywirusowy z ochroną plików w czasie rzeczywistym, bazy programu powinny być aktualizowane codziennie. Dodatkowo zasoby komputerów powinny być okresowo sprawdzone na obecność wirusów.

3. Korzystanie z dyskietek i płyt CD musi być poprzedzone sprawdzeniem tych nośników programem antywirusowym.

4. Czynności związane z porządkowaniem zasobów (skanowanie, defragmentacja, usuwanie zbędnych plików) powinny być wykonywane okresowo,

5. Przetwarzane dane należy chronić przed nieuprawnionym dostępem.

6. Kopie awaryjne nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory eksploatowane na bieżąco.

7. Kopie awaryjne należy chronić przed nieuprawnionym dostępem i usuwać po ustaniu ich użyteczności.

8. Pracownikom wolno używać zainstalowanego oprogramowania wyłącznie zgodnie z instrukcją obsługi, warunkami licencji i bezpieczeństwa przetwarzania danych.

9. Pracownikom Urzędu Gminy Boleszkowice nie wolno użytkować sprzętu komputerowego, nośników, baz danych oraz oprogramowania nielegalnego i niezwiązanego z wykonywaną pracą.

10. Pracownikom nie wolno samodzielnie instalować żadnego oprogramowania.

11. Pracownicy winni wykorzystywać sprzęt komputerowy bazy danych i oprogramowanie funkcjonujące w Urzędzie Gminy Boleszkowice tylko w celach służbowych, zgodnie z przeznaczeniem i obowiązującymi przepisami prawnymi.

12. Pracownicy Urzędu Gminy Boleszkowice wykorzystujący w swojej pracy sprzęt komputerowy powinni utrzymywać go w należytym stanie technicznym wykorzystywać tylko urządzenia, oprogramowanie i nośniki służbowe.

13. Wszelkie awarie sprzętu komputerowego i oprogramowania pracownicy zobowiązani są zgłaszać niezwłocznie informatykowi. Tylko informatyk jest upoważniony do usunięcia awarii.

14. Aktualizacje programów przetwarzających dane osobowe przeprowadza informatyk.

15. Osoby korzystające ze służbowych komputerów przenośnych pracujących poza Urzędem są szczególnie zobowiązane do ochrony komputera. Na komputerach tych nie mogą znajdować się dane objęte ochroną.

16. Pracownicy mogą korzystać jedynie z oficjalnych skrzynek pocztowych, zabrania się korzystania z prywatnych skrzynek oraz innych komunikatorów elektronicznych.

17. Po zakończeniu pracy stacja robocza powinna zostać wyłączona.

ROZDZIAŁ XVIII

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub innego zbioru danych osobowych 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. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.

3. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

4. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. z 2004 r., Nr 100, poz. 1023).
5. Niniejsza "Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Boleszkowice" wchodzi w życie z dniem jej podpisania przez Wójta.