BURMISTRZ
MIASTA I GMINY
Bierutów

Zarządzenie nr 20/09
Burmistrza Miasta i Gminy Bierutów
z dnia 5 marca 2009 r.

w sprawie: wprowadzenia Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie.

Na podstawie art. 31 oraz art. 33 ust. 3 w związku z art.11a ust.1 pkt 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142 poz. 1591 ze zm.), art. 36. ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, ze zm.) oraz §3 i §4 ust.1 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) zarządzam co następuje:

§1.

1. Wprowadzam do stosowania „Politykę Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie." w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.
2. Wprowadzam do stosowania „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie" w brzmieniu stanowiącym załącznik nr 2 do niniejszego zarządzenia.

§2.

Zobowiązuje się Kierowników Referatów, osoby zatrudnione na samodzielnych stanowiskach pracy w tut. Urzędzie do sprawowania nadzoru nad ochroną przetwarzanych danych osobowych oraz do współpracy z Administratorem Bezpieczeństwa Informacji (dalej: ABI) w tym zakresie oraz z Administratorem Systemu Informatycznego do przetwarzania danych osobowych (dalej: ASI).

§3.

Zobowiązuje się pracowników Urzędu Miasta i Gminy w Bierutowie przetwarzających dane osobowe, do przestrzegania przepisów o których mowa w § 1.

§4.

Wykonanie zarządzenia powierzam Sekretarzowi Miasta i Gminy Bierutów.

§5.

Traci moc Zarządzenie nr 14/99 Burmistrza Miasta i Gminy Bierutów z dnia 1 października 1999 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych systemów informatycznych służących do przetwarzania danych osobowych.

§6.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Miasta i Gminy Bierutów
Władysław Bogusław Kobiałka

Uzasadnienie
do Zarządzenia nr 20/09
Burmistrza Miasta i Gminy Bierutów
z dnia 05 marca 2009 r.

w sprawie: wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie.

Ustawa o ochronie danych osobowych oraz akty wykonawcze do tej ustawy nakładają na organ samorządu terytorialnego – Administratora Danych Osobowych obowiązek wprowadzenia Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
Po dokonaniu przeglądu Zarządzenia nr 14/99 z dnia 1 października 1999 r. stwierdziłem, że należy dokonać aktualizacji wprowadzonych dokumentów z uwzględnieniem reorganizacji Urzędu.

BURMISTRZ
Miasta i Gminy Bierutów
Władysław Bogusław Kobiałka

Załącznik nr 1 do Zarządzenia nr 20/09
Burmistrza Miasta i Gminy Bierutów z dnia 5 marca2009 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY W BIERUTOWIE

Spis treści:

Rozdział 1
Cel i zakres Polityki

1) „Polityka Bezpieczeństwa" zwana dalej Polityką, ma na celu określenie kierunków działania i postępowania dla zapewnienia bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie, zwanym dalej Urzędem.
2) „Polityka" stanowi wewnętrzny dokument wydany przez Burmistrza Miasta i Gminy w Bierutowie do stosowania przez wszystkich pracowników tut. Urzędu.
3) „Polityka" w zakresie przedmiotowym obejmuje zbiory danych osobowych, które przetwarzane są w tut. Urzędzie zarówno w formie elektronicznej, jak i tradycyjnej (papierowej), a dane gromadzone są w zbiorach ewidencyjnych, zbiorach danych zarówno w systemie informatycznym jak i poza nim.
4) „Polityka" w zakresie podmiotowym obowiązuje wszystkich pracowników tut. Urzędu oraz inne osoby mające dostęp do danych osobowych w Urzędzie, w tym stażystów, studentów odbywających praktyki, osoby zatrudnione na umowę zlecenie, umowę o dzieło.

Rozdział 2
Postanowienia ogólne

2.1. Podstawa Prawna.

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.) – zwana dalej ustawą.
2) Rozporządzenie 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).

2.2. Odpowiedzialność.

1) Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji, przyjmującego oznaczenie ABI, który jest odpowiedzialny za nadzór zgodnie z art. 36 ust. 3 ustawy, nad przestrzeganiem zasad ochrony. Odpowiedzialność ABI potwierdzona jest w stosownym upoważnieniu i zakresie jego czynności.
2) Do wspomagania pracy ABI, Administrator Danych wyznacza Administratora Systemu Informatycznego, przyjmującego skrót ASI, którego zadania i odpowiedzialność wynikają z niniejszego zarządzenia i potwierdzone są stosownym upoważnieniem.
3) Kierownicy Referatów, samodzielni pracownicy niezwłocznie zgłaszają ABI wszelkie zmiany w zbiorach danych osobowych oraz nowe lub wyrejestrowane zbiory danych osobowych, które zostały zgłoszone Generalnemu Inspektorowi Ochrony Danych Osobowych (*załącznik nr 1 do Polityki Bezpieczeństwa).*
4) Pracownik na stanowisku ds. Kadr tut. Urzędu zobowiązany jest zgłosić do ABI każdego nowo zatrudnionego pracownika, stażystę, praktykanta, celem przeprowadzenia szkolenia przez ABI, co pracownik potwierdza oświadczeniem stanowiącym (*załącznik nr 2 do Polityki Bezpieczeństwa).*
5) Przetwarzanie danych osobowych prowadzonych w postaci papierowej czy elektronicznej jest dopuszczone wyłącznie przez osoby posiadające upoważnienie wydane przez ABI i zaakceptowane w przypadku przetwarzania w systemie informatycznym przez ASI (*stanowiące załącznik nr 3 do Polityki Bezpieczeństwa).*

6) Kierownik lub bezpośredni przełożony pracownika występuje z wnioskiem (*załącznik nr 4 do Polityki Bezpieczeństwa)*, do ABI o wydanie dla pracownika upoważnienia (o którym mowa w punkcie 5), a w przypadku jeżeli dane przetwarzane są w systemie informatycznym również o przydzielenie uprawnień w systemie informatycznym.
7) Kierownik lub bezpośredni przełożony pracownika występuje niezwłocznie z wnioskiem (*załącznik nr 4 do Polityki Bezpieczeństwa)*, do ABI o odebranie uprawnienia do przetwarzania danych osobowych pracownikowi upoważnionemu do przetwarzania danych osobowych. Ten fakt zaznacza ABI na wcześniej wydanym dokumencie (*załącznik nr 3 do Polityki Bezpieczeństwa*).
8) Każdy pracownik przetwarzający dane zobowiązany jest zapewnić ich należytą ochronę , przestrzegać zasad ochrony danych i zabezpieczeń danych, w tym również w systemie informatycznym.

2.3. Określenia i skróty użyte w Polityce bezpieczeństwa oznaczają:

1) **Urząd Miasta i Gminy w Bierutowie** – Urząd,
2) **Administrator Danych Osobowych** – Burmistrz Miasta i Gminy Bierutów zwany dalej Administratorem (art. 7 pkt 4 ustawy),
3) **Administrator Bezpieczeństwa Informacji**, zwany dalej **ABI** – osoba wyznaczona przez Administratora w rozumieniu art. 36 ust. 3 ustawy,
4) **Administrator Systemu Informatycznego**, zwany dalej **ASI** – osoba wyznaczona przez Administratora, odpowiedzialna za sprawność i konserwacje oraz wdrażanie i stosowanie zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe w zbiorach komórek organizacyjnych Urzędu Miasta i Gminy w Bierutowie,
5) **Osoba upoważniona** lub **użytkownik systemu**, zwany dalej użytkownikiem – osoba posiadająca upoważnienie wydane przez Administratora lub osobę wyznaczoną przez niego i dopuszczona, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej,
6) **Przełożony użytkownika**, zwany dalej przełożonym – kierownik komórki organizacyjnej Urzędu, bezpośredni przełożony odpowiedzialny za przestrzeganie zasad przetwarzania i ochrony danych osobowych przez podległych pracowników,
7) **Osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu Administratora. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Administratora podejmująca czynności w zakresie przekraczającym ramy jego upoważnienia,
8) **System informatyczny**, zwany dalej systemem - to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych (art. 7 pkt 2a ustawy),
9) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią (art. 7 pkt 2b ustawy),
10) **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie (art. 7 pkt2 ustawy),
11) **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych wg określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielny funkcjonalnie (art. 7 pkt 1 ustawy).

Rozdział 3
Wykaz budynków, pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

1) Obszar przetwarzania danych osobowych w Urzędzie stanowi budynek Urzędu przy ul. Moniuszki 12 w Bierutowie:
   a) w piwnicy Urzędu znajduje się pomieszczenie serwerowni,
   b) na parterze budynku – dane przetwarzane są w postaci papierowej lub elektronicznej. Znajduje się tu Urząd Stanu Cywilnego i archiwum, w którym przechowywane są dokumenty USC,
   c) na I piętrze - dane przetwarzane są w postaci papierowej i elektronicznej,
   d) na strychu znajduje się archiwum zakładowe, w którym przechowywane są dokumenty Urzędu.
2) Kierownicy komórek organizacyjnych, samodzielni pracownicy zobowiązani są do dokonywania aktualizacji obszaru, w którym przetwarzane są dane osobowe oraz do zgłaszania zmian do ABI. ASI określa poziom bezpieczeństwa oraz system informatyczny, w przypadku przetwarzania zbioru w systemie informatycznym.
3) Szczegółowy wykaz obszarów przetwarzania zbiorów danych osobowych stanowi załącznik nr 5 do niniejszej Polityki.

Rozdział 4
Wykaz zbiorów danych osobowych.

1) Wykaz zbiorów danych osobowych zawiera *Załącznik nr 5* do niniejszej Polityki.
2) Nadzór na opracowaniem należy do obowiązków ABI, opracowany i aktualizowany jest na podstawie zgłoszeń kierowników komórek organizacyjnych oraz ASI szczególnie w zakresie systemów informatycznych.
3) Pierwszą stronę załącznika nr 5 stanowi „Karta zmian", na której dopuszcza się zaznaczanie bieżących zmian w zbiorach danych w zakresie objętym w załączniku. Zmian może dokonać w taki sposób ABI.

Rozdział 5
Opis struktury zbiorów.

1) Opisu struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań miedzy nimi dokonuje ABI lub inny wskazany przez ABI pracownik.

2) Opisu, o którym mowa w pkt 1 w odniesieniu do zbiorów danych przetwarzanych w systemach informatycznych dokonuje ASI.

3) Opis struktury zbiorów danych osobowych przetwarzanych w Urzędzie zawarty jest w *Załączniku Nr 5* do niniejszej Polityki.

Rozdział 6
Sposób przepływu danych pomiędzy poszczególnymi systemami służącymi do przetwarzania danych osobowych.

1) Główny zbiór danych osobowych **„Ewidencja ludności i dowodów osobistych"** obsługiwany jest za pomocą Systemu Ewidencji Ludności (ELUD). Dane nanoszone są na podstawie aktów Urzędów Stanu Cywilnego oraz udokumentowanych zgłoszeń mieszkańców gminy.
2) W Urzędzie funkcjonuje elektroniczny obieg dokumentów umożliwiający kontrolę przepływu dokumentów oparty o Rzeczowy Wykaz Akt.
3) Zbiory danych osobowych prowadzone w formie papierowej aktualizowane są na podstawie stosownych zaświadczeń oraz dokumentów.

Rozdział 7
Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1) Środki ochrony fizycznej:
   - Budynek Urzędu poza godzinami pracy nadzorowany jest przez pracowników zewnętrznej firmy zajmującej się ochroną osób i mienia,
   - urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami.
2) Środki sprzętowe i informatyczne:
   - zastosowano niszczarki dokumentów,
   - dane są przetwarzane w sposób zdecentralizowany,
3) Środki ochrony w ramach oprogramowania systemu:
   - dostęp fizyczny do baz danych osobowych zastrzeżony jest dla ABI oraz ASI,
   - konfiguracja systemu umożliwia użytkownikom dostęp do danych osobowych tylko za pośrednictwem aplikacji;
   - systemy operacyjne serwerów pozwalają zdefiniować prawa dostępu do określonych zasobów,
   - zastosowano działające w „tle" programy antywirusowe na komputerach użytkowników;
   - zastosowano programy antywirusowe działające na serwerach;
   - zablokowanie dostępu pracownikom do stron internetowych mogących naruszyć funkcjonowanie wewnętrznego systemu komputerowego.
4) Środki ochrony w ramach narzędzi baz danych:
   - automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego lub przeglądającego dane,
   - dla każdego użytkownika jest ustalony odrębny identyfikator i hasło,
   - zdefiniowano użytkowników oraz ich prawa dostępu do danych osobowych.

5) Środki organizacyjne:
   - wyznaczono Administratora Bezpieczeństwa Informacji - ABI ,
   - wyznaczono Administratora Systemu Informatycznego – ASI,
   - osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych oraz procedur przetwarzania danych,
   - prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,

- wprowadzono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do Zarządzenia Nr 20/09 Burmistrza Miasta i Gminy Bierutów dnia 5 marca 2009 r.,
- zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych, które zawarte są w niniejszej Polityce.

Rozdział 8
Naruszenie ochrony danych osobowych.

1) Naruszenie ochrony danych osobowych, może być spowodowane:
   a) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.,
   b) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu,
   c) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe lub osób odpowiedzialnych za ich ochronę.
2) Za naruszenie ochrony danych osobowych uważa się w szczególności:
   a) brak możliwości fizycznego dostępu do danych np. zagubiony klucz do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego itp.,
   b) brak dostępu do zawartości zbioru danych – zbiór istnieje lecz nie można go otworzyć,
   c) zmienioną zawartość zbioru, niepoprawną treść, postać, data, różnicę w danych itp.,
   d) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów,
   e) różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji,
   f) zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych,
   g) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych,
   h) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione,
   i) próba nielegalnego logowania się do systemu lub włamania do systemu,
   j) zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych,
   k) inne zdarzenie mogące mieć wpływ na niekontrolowaną zmianę zbioru danych osobowych.
3) Niniejsze zasady stosuje się także w przypadku stwierdzenia, że stan pomieszczeń i szaf, bądź mebli biurowych, w których przechowuje się dokumentację lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby trzecie.

Rozdział 9
Zabezpieczenie przed naruszeniem obszaru przetwarzania danych osobowych.

1) Dane osobowe przetwarza się w budynkach, pomieszczeniach lub częściach pomieszczeń, tworzących obszar wskazany w Załączniku nr 5 do niniejszej Polityki.
2) Budynki lub pomieszczenia, w których przetwarzane są dane, powinny być zamykane na czas nieobecności użytkowników, w sposób uniemożliwiający do nich dostęp osób trzecich.
3) Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczania na swoich stanowiskach pracy.
4) Klucze do pomieszczeń służbowych, przed rozpoczęciem i po zakończeniu pracy winny być odbierane i zdawane w sekretariacie na I piętrze w zamykanej metalowej gablocie, do której dostęp ma tylko upoważniony pracownik sekretariatu i pracownik gospodarczy.
5) Kierownicy komórek organizacyjnych sprawują kontrolę nad prawidłowym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe.

Rozdział 10
Kontrola przestrzegania zasad zabezpieczenia systemu ochrony danych osobowych.

1) Codzienną kontrolę w zakresie ochrony danych osobowych sprawuje użytkownik.
2) Nadzór nad przestrzeganiem zasad ochrony danych osobowych w danej komórce organizacyjnej sprawuje przełożony.
3) ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych w Urzędzie.
4) ASI dokonuje stałych kontroli i oceny funkcjonowania mechanizmów technicznych zabezpieczeń systemów, w których przetwarzane są dane osobowe. O przeprowadzonych kontrolach informuje ABI.

Rozdział 11
Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych.

1) W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w rozdziale 8 niniejszej Polityki, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz ABI lub osobę upoważnioną przez ABI.
2) Użytkownik do momentu przybycia ABI, lub osoby przez niego upoważnionej powinien:
   a) zabezpieczyć dostęp do pomieszczenia lub urządzenia,
   b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony,
   c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony,
   d) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.
3) ASI po otrzymaniu informacji o naruszeniu lub próby naruszenia zabezpieczenia systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia.
4) Po przybyciu na miejsce, ASI realizuje czynności w kolejności:

a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych,
b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia,
c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony,
d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń,
e) biorąc pod uwagę skalę oraz skutki naruszenia ochrony, ABI decyduje o powołaniu doraźnego zespołu i powiadomieniu o zdarzeniu Administratora lub osobę upoważnioną przez niego.

5) ASI z przebiegu zdarzenia sporządza notatkę służbową, która obejmuje:
a) dane osoby stwierdzającej naruszenie ochrony
b) datę, godzinę i miejsce naruszenia ochrony,
c) rodzaj naruszenia ochrony,
d) czas powiadomienia o zdarzeniu,
e) opis podjętych czynności,
f) wnioski do realizacji.

6) Notatkę otrzymaną od ASI, ABI przekazuje Administratorowi lub osobie upoważnionej przez niego.

7) Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych, wyraża ABI lub osoba przez niego upoważniona.

8) Dokonywanie zmian w miejscu naruszenia ochrony bez zgody, o której mowa w pkt 7 jest dopuszczalne tylko w wypadku konieczności ratowania osób, mienia albo zapobieżenia powstaniu innego niebezpieczeństwa.

9) W przypadku powołania doraźnego zespołu, jego pracami kieruje ABI:
a) Zespół z przeprowadzonych czynności sporządza protokół, w którym ujmuje skalę stwierdzonych naruszeń ochrony, przyczyny ich powstania oraz skutki jakie wpłynęły lub wpłynąć mogą na stan zabezpieczenia i ochrony danych osobowych.
b) Protokół zawierać powinien wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości naruszeniom ochrony danych osobowych.
c) Protokół przekazywany jest Administratorowi lub osobie upoważnionej przez niego w celu akceptacji wniosków i zaleceń usprawniających zabezpieczenia ochrony danych.

10. W przypadku stwierdzenia:
a) błędu użytkownika systemu – ASI przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej,
b) uaktywnienia wirusa – należy zgłosić ASI, który ustali źródło jego pochodzenia oraz uaktualni zabezpieczenia antywirusowe,
c) zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa,
d) włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę,
e) złego stanu urządzenia lub złego działania programu – należy niezwłocznie powiadomić ASI i przeprowadzić kontrolę czynności serwisowo-programowych.

Rozdziała 12
Postanowienia końcowe

1) Każdy użytkownik przetwarzający dane osobowe w zbiorach Urzędu zobowiązany jest zapoznać się z niniejszą Polityką i stosować przepisy w niej zawarte na swoim stanowisku pracy.
2) Nadużycie przez użytkownika postanowień niniejszej Instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

Rozdział 13
Załączniki

1) Informacja o zmianach dotycząca zbioru danych osobowych *(dotyczy kierownika , samodzielnego pracownika lub bezpośredniego przełożonego).*
2) Oświadczenie pracownika o zapoznaniu się z obowiązującymi przepisami z zakresu ochrony danych osobowych *(dotyczy każdego pracownika)*
3) Zaświadczenie - upoważnienie do przetwarzania danych *(wystawia ABI, ASI na wniosek kierownika, samodzielnego pracownika lub bezpośredniego przełożonego).*
4) wniosek o upoważnienie do przetwarzania danych osobowych oraz przydzielenia uprawnień w systemie informatycznym *(do ABI składa kierownik, samodzielny pracownik lub bezpośredni przełożony).*
5) wykaz zbiorów danych osobowych i obszar ich przetwarzania.

Załącznik Nr 1 do „ Polityki Bezpieczeństwa"
(Zarządzenie Nr 20/09 Burmistrza Miasta i Gminy Bierutów z dnia 5 marca 2009 r.)

Bierutów, ...

Administrator Bezpieczeństwa Informacji
Urząd Miasta i Gminy w Bierutowie

I N F O R M A C J A
O ZMIANACH DOTYCZĄCYCH
ZBIORU DANYCH OSOBOWYCH

1. Informuję , że zmienił się:
   a) opis struktury zbiorów danych osobowych,
   b) obszar, gdzie przetwarzane są dane,
   c) program komputerowy *(w tym również przejście z papierowego zbioru na informatyczny,)*
   d) inne *(jakie?)*.....

2. Informuję , że zgłoszono nowy zbiór do GIODO

   o nazwie.....

3. Informuję , że zgłoszono wniosek do GIODO o wyrejestrowanie zbioru

   o nazwie .....

.....
podpis Kierownika komórki organizacyjnej

Załącznik Nr 2 do „ Polityki Bezpieczeństwa"
(Zarządzenie Nr 20/09 Burmistrza Miasta i Gminy Bierutów z dnia 5 marca 2009 r.)

Bierutów, dnia .....

.....
(imię i nazwisko pracownika)

.....
(stanowisko i nazwa komórki organizacyjnej)

OŚWIADCZENIE

Oświadczam, że uczestniczyłem/łam w szkoleniu z zakresu danych osobowych, zapoznałem/łam się z przepisami dotyczącymi ochrony danych osobowych oraz o przyjęciu do wiadomości obowiązku zachowania tajemnicy i zobowiązuję się do przestrzegania:

1. Ustawy z dni 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101 poz. 926 ze zm.).
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr 100 poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych .
3. „Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie".
4. „Polityki Bezpieczeństwa" Urzędu Miasta i Gminy w Bierutowie.

<u>Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:</u>

a) zapewnienia ochrony danych osobowych przetwarzanych w zbiorach Urzędu Miasta i Gminy w Bierutowie, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
b) zachowaniem w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych w zbiorach Urzędu Miasta i Gminy w Bierutowie.
c) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Miasta i Gminy w Bierutowie, również po upływie jego ważności,
d) natychmiastowego zgłaszania przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia, na swoim stanowisku pracy, próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru lub systemu informatycznego, w którym przetwarzane są dane osobowe.

.....
(podpis pracownika ubiegającego się o dostęp)

Załącznik Nr 3 do „ Polityki Bezpieczeństwa"
(Zarządzenie Nr 20/09 Burmistrza Miasta i Gminy Bierutów z dnia 5 marca 2009 r.)

Bierutów, dnia .....

Z A Ś W I A D C Z E N I E

- **o dostępie do przetwarzania danych osobowych w zbiorach Urzędu ***
- **o dostępie do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe w zbiorach Urzędu***
- **o zakresie przetwarzania danych osobowych w zbiorach w celach innych niż włączenie do zbioru ***

Zaświadcza się, że Pan(i):

.....

na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.) otrzymał(a) upoważnienie do przetwarzania danych osobowych w zbiorach Urzędu Miasta i Gminy w Bierutowie, w zakresie merytorycznej działalności komórki organizacyjnej.

zapoznał(a) się z obowiązującymi przepisami dotyczącymi ochrony danych osobowych, jest uprawniona do przetwarzania danych osobowych w zbiorze o nazwie:

.....

Pouczenie:
Zaświadczenie jest ważne na czas zatrudnienia na danym stanowisku. Po ustaniu zatrudnienia, zmiany stanowiska należy je zwrócić kierownikowi komórki organizacyjnej.

.....
Administrator Systemów Informatycznych

.....
Administrator Bezpieczeństwa Informacji

Załącznik Nr 4
do „ Polityki Bezpieczeństwa"
(Zarządzenie Nr 20/09 Burmistrza Miasta i Gminy Bierutów z dnia 5 marca 2009 r.)

Bierutów, dn. .....

.....
(pieczęć komórki organizacyjnej)

Administrator Bezpieczeństwa Informacji
Urzędu Miasta i Gminy w Bierutowie

W N I O S E K

Na podstawie Rozdziału 2, ust 2.2 pkt 6 „Polityki Bezpieczeństwa" Urzędu Miasta i Gminy w Bierutowie, wnioskuję o **udzielenie / (pozbawienie)***

Pani /Pana/* .....

a) dostępu do przetwarzania danych osobowych w komórce organizacyjnej Urzędu Miasta i Gminy w Bierutowie z powodu: (*przyjęcia do pracy, przejścia na inne stanowisko, zwolnienia z pracy)* lub innego (jakiego?)*.....

b) dostępu do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe (*przyjęcia do pracy, przejścia na inne stanowisko, zwolnienia z pracy)* lub innego (jakiego?)*
.....

1. Nazwa zbioru danych osobowych .....

2. Uprawnienia: (*dostępu do przetwarzania)*, (rozpatrywania wniosków)* (użytkownika systemu)*, z tytułu zajmowanego stanowiska (jakiego?)*
   .....

3. Sposób przetwarzania danych osobowych: *papierowy/ informatyczny/**

4. Miejsce przetwarzania danych osobowych (adres siedziby)
   *Urząd Miasta i Gminy w Bierutowie: ul. Moniuszki 12 /56-420 Bierutów/**

   obszar (piętro, nr pokoju) .....

5. Zobowiązano pracownika do podpisania oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych: *tak/ nie**

.....
(kierownik komórki organizacyjnej)

/* niepotrzebne proszę skreślić

Załącznik nr 5 do Polityki Bezpieczeństwa
(Zarządzenie Nr 20/09 Burmistrza Miasta i Gminy Bierutów z dnia 5 marca 2009 r.)

WYKAZ ZBIORÓW DANYCH OSOBOWYCH I OBSZAR ICH PRZETWARZANIA

Lp.	Nazwa zbioru danych	Komórka organizacyjna	Podstawa prawna	Forma	Zakres przetwarzanych danych osobowych	Pomieszczenia, w których przetwarzane są dane	Opiekun zbioru	Wymóg zgłoszenia do GIODO
1.	**Ewidencja ludności i dowodów osobistych**	SO	Ustawa o Ewidencji Ludności	**P**- Karta Osobowa Mieszkańca **E**- Sys. Ewidencji Ludności	- nr ewidencyjny PESEL - imię i nazwisko - adres (kod terytorialny, miejscowość, ulica, nr domu, nr mieszkania, kod pocztowy) - rodzaj zameldowania (data zameldowania, data wymeldowania) - płeć - nazwisko rodowe - imię ojca - nazwisko ojca - nazwisko rodowe ojca - imię matki - nazwisko rodowe matki - dane o urodzeniu (data, miejsce urodzenia, USC- kod terytorialny, nr aktu urodzenia, data wystawienia) - stan cywilny (data zmiany, organ – kod terytorialny, nazwa organu, nr akt, współmałżonek-nazwisko, imię, PESEL, forma ustania małżeństwa) - dokument tożsamości (seria i numer, data wystawienia, wystawca-kod terytorialny, nazwa wystawcy) - rysopis (wzrost w cm, kolor oczu, znak szczególny) - obowiązek wojskowy (dokument wojskowy, seria i numer, stopień wojskowy) - obywatelstwo obce (data zmiany, podstawa prawna zmiany) - data zgonu (USC aktu zgonu, nr aktu zgonu) - grupa krwi - uprawnienia wyborcze - status mieszkańca - data wprowadzenia rekordu - data ostatniej modyfikacji - czasokres nieobecności (pobyt czasowy) - data zgonu.	pok. Nr 2, budynek A	Ewa Słomska, Monika Krosta,	
2.	**Archiwum kopert dowodowych (anulowanych dowodów**	SO	Ustawa o Ewidencji Ludności	**P**		pok. Nr 2, budynek A pomieszczenia USC	Ewa Słomska	

	osobistych)					przy ul. Moniuszki 12 w Bierutowie		
3.	**Akta stanu cywilnego**	USC	Ustawa prawo o aktach stanu cywilnego Kodeks rodzinny i opiekuńczy Ustawa o zmianie imion i nazwisk	**P**	***akt urodzenia:*** - dane dotyczące dziecka (nazwisko, imię, data urodzenia, miejsce urodzenia) - dane dotyczące rodziców (nazwisko ojca, imię ojca, nazwisko rodowe ojca, data urodzenia ojca, miejsce urodzenia ojca, miejsce zamieszkania ojca, nazwisko matki, nazwisko rodowe matki, data urodzenia matki, miejsce urodzenia matki, miejsce zamieszkania matki) - dane dotyczące osoby/zakładu zgłaszającej urodzenie (nazwisko i imię lub nazwa, miejsce zamieszkania lub siedziba) ***akt małżeństwa:*** - dane dotyczące osób zawierających małżeństwo (nazwisko, imię, nazwisko rodowe, stan cywilny, data urodzenia, miejsce urodzenia, miejsce zamieszkania) - dane dotyczące daty i miejsca zawarcia małżeństwa (data, miejsce) - dane dotyczące rodziców (nazwiska, imiona, nazwiska rodowe) - nazwisko noszone po zawarciu małżeństwa (mężczyzny, kobiety, dzieci) - świadkowie (nazwisko, imię) ***akt zgonu:*** - dane dotyczące osoby zmarłej (nazwisko, imię, nazwisko rodowe, stan cywilny, data urodzenia, miejsce urodzenia, ostatnie miejsce zamieszkania) - dane dotyczące daty i miejsca zgonu (data zgonu, godzina zgonu, data znalezienia zwłok, godzina znalezienia zwłok, miejsce znalezienia zwłok) - dane dotyczące małżonka osoby zmarłej (nazwisko i imię, nazwisko rodowe) - dane dotyczące rodziców osoby zmarłej (imiona, nazwiska rodowe) - dane dotyczące osoby/zakładu zgłaszającej urodzenie (nazwisko i imię lub nazwa, miejsce zamieszkania lub siedziba)	pok. Nr 2, budynek A pomieszczenia USC przy ul. Moniuszki 12 w Bierutowie	Ewa Słomska	
4.	**Świadczenia osobiste na rzecz obrony kraju**	SO	Ustawa o powszechnym obowiązku obrony Rzeczpospolitej Polskiej	**P**	- nr decyzji - nr wezwania - znak sprawy - świadczeniobiorca	pok. nr 13, budynek A	Grzegorz Marciniak	

			Rozporządzenie w sprawie świadczeń osobistych na rzecz obrony w czasie pokoju		- nazwa świadczeniodawca (imię, nazwisko lub nazwa zakładu)			
5.	**Świadczenia rzeczowe na rzecz obrony kraju**	SO	Ustawa o powszechnym obowiązku obrony Rzeczpospolitej Polskiej Rozporządzenie w sprawie świadczeń rzeczowych na rzecz obrony w czasie pokoju	**P**	- nr decyzji - nr wezwania - znak sprawy - świadczeniobiorca - nazwa lub imię - nazwisko świadczeniodawcy - uwagi	pok. nr 13, budynek A	Grzegorz Marciniak	
6.	**Wykaz osób o nieuregulowanym stosunku do służby wojskowej**	SO	Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. Rozporządzenie w sprawie przygotowania i przeprowadzenia poboru Rozporządzenie w sprawie rejestracji przedpoborowych.	**P**	- liczba porządkowa z wykazu przedpoborowych - liczba porządkowa z listy poborowych - PESEL - nazwisko i imię - imiona rodziców - data urodzenia - miejsce zamieszkania - rodzaj pobytu - wyznaczona data stawienia się do: rejestracji, poboru - przyczyny niezgłoszenia się - faktyczna data zgłoszenia się do: rejestracji, poboru - miejsce zgłoszenia się do: rejestracji, poboru - seria i numer książeczki wojskowej oraz WKU - zastosowane sankcje karne - podstawa skreślenia	pok. nr 13, budynek A	Grzegorz Marciniak	
7.	**Lista poborowych**	SO	Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej Rozporządzenie w sprawie przygotowania i przeprowadzenia poboru.	**P**	- nr z księgi orzeczeń lekarskich - nazwisko i imię - imię ojca - rok urodzenia - miejsce stałego lub czasowego pobytu (adres) - data stawienia się do poboru - kategoria - seria i numer książeczki wojskowej - uwagi, adnotacje dot. przyczyn dopisania lub skreślenia z listy	pok. nr 13, budynek A	Grzegorz Marciniak	
8.	**Rejestr przedpoborowych**	SO	Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. Rozporządzenie w sprawie rejestracji przedpoborowych.	**P**	- nazwisko i imię - imię ojca - rok urodzenia - seria i nr dowodu osobistego - adres pobytu - data zameldowania - miejsce poprzedniego pobytu - data wymeldowania - miejsce nowego pobytu - data zgłoszenia się do rejestracji - pokwitowanie odbioru potwierdzenia - data zgłoszenia się do poboru - nr książeczki wojskowej	pok. nr 13, budynek A	Grzegorz Marciniak	

9.	**Wykaz przedpoborowych**	SO	Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. Rozporządzenie w sprawie rejestracji przedpoborowych.	**P**	- nazwisko i imię - imię ojca - rok urodzenia - seria i nr dowodu osobistego - adres pobytu - miejsce aktualnego pobytu stałego, czasowego - wezwano na dzień - zgłosił się dnia - nr pozycji w rejestrze przedpoborowych	pok. nr 13, budynek A	Grzegorz Marciniak	
10.	**Rejestr umów i zleceń**	ORG	Ustawa prawo zamówień publicznych. Ustawa o ochronie danych osobowych.	**P**	- numer nadany przez referat - imię i nazwisko oraz adres zleceniobiorcy - zadanie do wykonania - data rejestracji umowy	pok. nr 14, budynek A	Małgorzata Rębielak	
11.	**Rejestr kancelaryjny**	ORG	Ustawa o samorządzie gminnym. Rozporządzenia Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych	**P** **E** – System Obiegu Dokumentów i Spraw mis-Partner21/Urzędy	- nazwisko - imię 1 - imię 2 - PESEL - NIP - Miejscowość - nr domu - nr lokalu - kod pocztowy - poczta - kraj - województwo - powiat - gmina	pok. nr 14, budynek A	Małgorzata Rębielak	
12.	**Rejestr skarg i wniosków**	ORG	Rozporządzenie Rady Ministrów w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków Kodeks postępowania administracyjnego Rozporządzenie Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych.	**P**	- nr skargi/wniosku - data wpływu - skąd otrzymano - nazwisko i imię oraz adres - treść skargi, wniosku lub listu - miejsce przekazania - data przekazania - termin udzielenia odpowiedzi - sposób załatwienia - data otrzymania odpowiedzi	pok. nr 14, budynek A	Małgorzata Rębielak	
13.	**Rejestr wniosków o udostępnienie informacji publicznej**	ORG	Ustawa o dostępie do informacji publicznej.	**P**	- data - dane wnioskodawcy - temat wnioskowanej informacji - wydział/referat - sposób udzielenia odpowiedzi - data wysłania	pok. nr 14, budynek A	Małgorzata Rębielak	

14.	**Ewidencja kadrowo-pracownicza**	ORG (Kadry)	Kodeks pracy Ustawa o pracownikach samorządowych Ustawa o promocji zatrudnienia i instytucjach rynku pracy.	**P** **E** – R2 Płatnik	- nr akt - PESEL - NIP - nazwisko - imię - data urodzenia - gmina - miejsce zamieszkania - ulica - nr domu - nr mieszkania - kod pocztowy - rodzaj dokumentu - nr dokumentu - wydawca dowodu - data wydania dowodu - telefon - nr akt - nazwisko rodowe - płeć - miejsce urodzenia - imię ojca - imię matki - stan cywilny - obowiązek wojskowy - rodzaj dokumentu - nr książeczki wojskowej - stopień wojskowy - obywatelstwo - wykształcenie - data stażu - tytuł - zawód wyuczony - zawód wykonywany - tryb nawiązania pracy - początek zatrudnienia - koniec zatrudnienia - data zatrudnienia - umowa - stanowisko - wymiar czasu pracy	pok. nr 6, budynek A	Karolina Jaśko	
15.	**Dane dyrektorów jednostek organizacyjnych**	ORG (Kadry)		**P**	- nr akt - PESEL - NIP - Nazwisko - Imię - data urodzenia - gmina - miejsce zamieszkania - ulica - nr domu - nr mieszkania - kod pocztowy - rodzaj dokumentu - nr dokumentu - wydawca dowodu	pok. nr 6, budynek A	Karolina Jaśko	

					- data wydania dowodu - telefon - nr akt - nazwisko rodowe - płeć - miejsce urodzenia - imię ojca - imię matki - stan cywilny - obowiązek wojskowy - rodzaj dokumentu - nr książeczki wojskowej - stopień wojskowy - obywatelstwo - wykształcenie - data stażu - tytuł - zawód wyuczony - zawód wykonywany - tryb nawiązania pracy - początek zatrudnienia - koniec zatrudnienia - data zatrudnienia - umowa - stanowisko - wymiar czasu pracy			
16.	**Rejestry kadrowe:** **Dane stażystów i praktykantów** **Dane zawarte w oświadczeniach majątkowych** **Rejestr upoważnień**	ORG (Kadry)		**P**	- nazwisko - imię - data urodzenia - gmina - miejsce zamieszkania - ulica - nr domu - nr mieszkania - kod pocztowy	pok. nr 6, budynek A	Karolina Jaśko	

17.	**Podatek rolny** **Podatek leśny** **Podatki i opłaty lokalne**	FN FN FN	Ustawa o podatku rolnym. Ustawa o podatku leśnym. Ustawa o podatkach i opłatach lokalnych	**P** **E** - System Naliczania Podatków od Gruntów i Nieruchomości (program księgowy ADAS) **P** **E** - System Naliczania Podatków od Gruntów i Nieruchomości (program księgowy ADAS) **P** **E** - System Naliczania Podatków od Gruntów i Nieruchomości, podatku od środków transportowych (program księgowy ADAS)	- nazwisko - imię - data urodzenia - imię ojca - imię matki - kod pocztowy - miejscowość - ulica - nr domu - nr lokalu - PESEL - NIP - Rejon - dane dotyczące przedmiotu opodatkowania (powierzchnia gruntów, powierzchnia użytkowa budynków lub ich części, budowle, informacja o przedmiotach i podmiotach zwolnionych, miejsce położenia nieruchomości, samochody ciężarowe, przyczepy, naczepy)	pok. nr 1, budynek A	Ewa Pelikan Janina Knefel	
18.	**Rejestr decyzji w sprawach z zakresu ochrony środowiska**	GŚ	Ustawa prawo ochrony środowiska Ustawa prawo geologiczne i górnicze Ustawa o odpadach	**P**	- nazwisko - imię - data urodzenia - imię ojca - imię matki - kod pocztowy - miejscowość - ulica - nr domu - nr lokalu - PESEL	Pok. Nr 15, budynek B Pok. Nr 17, budynek B Pok. Nr 17, budynek B	Jerzy Pęciak Barbara Łabuś Stanisław Paluch	
19.	**Gospodarka mieniem komunalnym**	GŚ	Ustawa o gospodarce nieruchomościami Ustawa o przekształceniu prawa użytkowania wieczystego w prawo własności Ustawa prawo geodezyjne i kartograficzne	**P** **E** - System Ewidencji Mienia Komunalnego (program księgowy ADAS)	- nr akt - imię - nazwisko - PESEL - kod pocztowy - miejscowość - ulica - nr domu - kwota - opis	Pok nr 16, budynek B Pok. Nr 17, budynek B	Waldemar Roniek Barbara Łabuś	

20.	**Rejestr osób uzależnionych**	ORG	Ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi	**P**	- nazwisko i imię - nr akt - rok założenia akt	Pok. nr 15, Budynek B	Magda Zganiacz	
21.	**Rejestr przedsiębiorców posiadających zezwolenie na sprzedaż napojów alkoholowych**	ORG	Ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi	**P**	- nr zezwolenia - adres punktu sprzedaży - rodzaj punktu sprzedaży - imię i nazwisko (lub nazwa) otrzymującego zezwolenie - adres otrzymującego zezwolenie - rodzaj wydanego zezwolenia - data wystawienia zezwolenia - termin ważności zezwolenia	Pok. nr 15, Budynek B	Magda Zganiacz	
22.	**Rejestr osób fizycznych prowadzących działalność gospodarczą**	ORG	Ustawa prawo działalności gospodarczej Ustawa o swobodzie działalności gospodarczej	**P** E- wykaz przedsiębiorców	- nr akt - nr ewidencyjny nazwa - adres - data rozpoczęcia - data zgłoszenia - data wpisu - data doręczenia - data decyzji - nr decyzji - data zawieszenia - data odwieszenia - PKD - nr sprawy - kod pocztowy	Pok. nr 15, Budynek B	Magda Zganiacz	
23.	**Zakładowy Fundusz Świadczeń Socjalnych**	FN	Ustawa o zakładowym funduszu świadczeń socjalnych	**P**	- nazwisko i imię - data urodzenia - uprawnienia do korzystania z Funduszu - stan cywilny - data przejścia na emeryturę, rentę - data, rodzaj i termin zatrudnienia - informacje o przyczynach pozbawienia prawa do korzystania z Funduszu - ewidencja korzystania z Funduszu	pok. nr 1, budynek A	Ewa Pelikan	
24.	**Kopie aktów notarialnych**	GŚ	Ustawa o gospodarce nieruchomościami Uchwała Rady Miejskiej w Bierutowie w sprawie określenia zasad sprzedaży lokali mieszkalnych stanowiących własność Gminy Bierutów Uchwała Rady Miejskiej w Bierutowie w sprawie określenia zasad wydzierżawiania nieruchomości	**P**	- imiona i nazwisko - adres zamieszkania - nr dowodu osobistego - imiona rodziców - NIP - PESEL	Pok nr 16, budynek B	Waldemar Roniek	

			gruntowych na okres nie dłuższy niż 3 lata.					
25.	**Wykaz radnych Rady Miejskiej w Bierutowie**	OR	Ustawa o samorządzie gminnym	**P**	- imię i nazwisko - adres zamieszkania - telefon kontaktowy	Pok. nr 12, budynek A	Iwona Wiśniewska-Kocjan	
26.	**Rejestr Sołtysów**	OR	Ustawa o samorządzie gminnym Uchwała Rady Miejskiej w Bierutowie w sprawie zarządzenia wyborów Sołtysa i Rady Sołeckiej	**P**	- imię i nazwisko - data urodzenia - miejsce zamieszkania - telefon - miejsce pracy	Pok. nr 12, budynek A	Iwona Wiśniewska-Kocjan	
27.	**Dane osób wynajmujących, dzierżawiących lokale mieszkalne, komórki, garaże** **Dane osób składających wniosek o przyznanie dodatku mieszkaniowego i osób którym organ przyznał dodatek mieszkaniowy**	IR GŚ	Ustawa o gospodarce nieruchomościami Uchwała Rady Miejskiej w Bierutowie w sprawie określenia zasad wydzierżawiania nieruchomości gruntowych na okres nie dłuższy niż 3 lata. Ustawa o dodatkach mieszkaniowych	**P**	- imię i nazwisko - data urodzenia - miejsce zamieszkania - telefon - miejsce pracy - wysokość osiąganych dochodów	Pok. Nr 14, budynek B Pok nr 16, budynek B	Janina Leszczyńska Waldemar Roniek Współpraca z RBK i ZWKiO	
28.	**Strony internetowe:** www.bierutow.pl							

P – papierowy
E- elektroniczny

Załącznik nr 2 do Zarządzenia nr 20/09
Burmistrza Miasta i Gminy Bierutów z dnia 5 marca 2009 r.

INSTRUKCJA
zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie

Spis treści

Rozdział 1
Postanowienia ogólne.

1) Niniejsza „Instrukcja określająca sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bierutowie", zwana dalej Instrukcją, jest dokumentem wewnętrznym wydanym przez Burmistrza Miasta i Gminy Bierutów i ma zastosowanie do przetwarzania danych osobowych w systemach informatycznych Urzędu, w celu bezpiecznego ich wykorzystywania.

2) Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych, osób wyznaczonych przez niego oraz wszystkich użytkowników, przetwarzających dane osobowe w systemach informatycznych Urzędu.

3) Instrukcja została opracowana zgodnie z wymogami § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).

4) Określenia i skróty użyte w Instrukcji oznaczają:
   a) **Urząd** - Urząd Miasta i Gminy w Bierutowie,
   b) **Administrator Danych Osobowych** – Burmistrz Miasta i Gminy Bierutów, zwany dalej Administratorem,
   c) **Administrator Bezpieczeństwa Informacji**, zwany dalej **ABI** – osoba wyznaczona przez Administratora w rozumieniu art.36 ust.3 ustawy,
   d) **Administrator Systemu Informatycznego**, zwany dalej **ASI** – osoba wyznaczona przez Administratora, odpowiedzialna za sprawność i konserwacje oraz wdrażanie zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe w zbiorach komórek organizacyjnych Urzędu,
   e) **Osoba upoważniona** lub **użytkownik systemu**, zwany dalej użytkownikiem – osoba posiadająca upoważnienie wydane przez Administratora lub osobę wyznaczoną przez niego i dopuszczona, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.
   f) **Przełożony użytkownika**, zwany dalej przełożonym – kierownik komórki organizacyjnej Urzędu,
   g) **Osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu Administratora. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Administratora podejmująca czynności w zakresie przekraczającym ramy jego upoważnienia.
   h) **System informatyczny**, zwany dalej systemem to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
   i) **Zabezpieczenie systemu informatycznego** – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią,

j) **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, wprowadzanie zmian, opracowywanie, udostępnianie i ich usuwanie.

5) ABI może zlecić innej osobie, zatrudnionej u Administratora wykonywanie określonych czynności, leżących w zakresie jego obowiązków. Osoba niezwłocznie informuje ABI o podjętych przez siebie czynnościach. Kontrola prawidłowości wykonywania należy do ABI.

Rozdział 2
Przydział haseł i identyfikatorów dla użytkowników.

1) Systemy informatyczne, w których przetwarza się dane osobowe w zbiorach Urzędu muszą być wyposażone w mechanizmy uwierzytelniające użytkownika oraz kontroli dostępu do nich przez upoważnione osoby.
   a) Hasła dostępu każdy uprawniony użytkownik systemu ustala sam i natychmiast zmienia w wypadku podejrzenia lub stwierdzenia ujawnienia ich osobom trzecim.
   b) Hasła dostępu użytkownika pokazywane są na ekranie monitora w formie niejawnej i mogą być znane tylko użytkownikowi.
   c) Hasła obowiązują 2 miesiące i zmienia je dany użytkownik wg wymagań aplikacji systemowych oraz używanych programów. Hasła administracyjne obowiązują 1 rok i zmienia je ASI w pierwszy tygodniu nowego roku kalendarzowego lub wg wymagań aplikacji systemowych.
   d) Osobą odpowiedzialną za techniczny sposób ustalania, przechowywania i wprowadzania haseł jest ASI, który określa w tym zakresie szczegółowe zasady w swoich wytycznych.

2) Identyfikator składa się z ciągu liter, cyfr lub naprzemiennie, pisany małymi lub dużymi literami. W przypadku nazwisk składających się z dwóch członów, pod uwagę jest brany tylko pierwszy człon nazwiska. Identyfikator po wylogowaniu danej osoby z systemu, nie może być przydzielony innemu użytkownikowi. Identyfikator wpisuje się do „Ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych". Informację o zmianach w tym zakresie nadzoruje ASI i przekazuje ABI.

3) Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał.

4) Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia starań, w celu uniemożliwienia zapoznania się z nimi osób trzecich, nawet po ustaniu ich ważności.

Rozdział 3
Rejestrowanie i wyrejestrowywanie użytkowników.

1) Rejestracji i wyrejestrowania użytkowników z systemu dokonuje ASI na podstawie informacji uzyskanej od przełożonego użytkownika, wprowadzając dane do ewidencji.

2) Ewidencja zawierać powinna:
   a) imię i nazwisko użytkownika,
   b) nazwę komórki organizacyjnej, w której jest zatrudniony,
   c) identyfikator,
   d) datę nadania uprawnień,
   e) datę odebrania uprawnień.

3) Jakakolwiek zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.

4) Zarejestrowanie użytkownika w systemie wymaga spełnienia następujących warunków:

a) Złożenie wniosku przez przełożonego do osoby upoważnionej przez Administratora o udzielenie wskazanej osobie dostępu do przetwarzania danych osobowych, według wzoru zwartego w Polityce Bezpieczeństwa,
b) Podpisanie przez osobę, ubiegającą się o dostęp, oświadczenia dotyczącego zapoznania się z przepisami o ochronie danych osobowych i zobowiązania do zachowania w tajemnicy informacji związanych z ich przetwarzaniem, według wzoru zawartego w Polityce Bezpieczeństwa,
c) Wydanie przez ABI lub osobę upoważnioną przez niego zaświadczenia, upoważniającego użytkownika do przetwarzania danych osobowych, według wzorów zawartych w Polityce Bezpieczeństwa,
d) Z chwilą zarejestrowania w systemie użytkownik jest informowany przez ASI o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.

5) Powyższe dokumenty, podlegają przechowaniu:
   a) wniosek przełożonego o udzielenie dostępu osobie w dokumentacji adresata,
   b) oryginał oświadczenia osoby ubiegającej się o dostęp w komórce kadrowej, a kopia oświadczenia w dokumentacji ABI,
   c) oryginał zaświadczenia o dostępie otrzymuje osoba upoważniona, a kopie trafiają do akt personalnych pracownika i dokumentacji ABI.

6) Użytkownika wyrejestrowuje się z systemu na wniosek przełożonego – po utracie uprawnień dostępu do przetwarzania danych. Bezpośredni przełożeni użytkownika zobowiązani są do przekazywania pisemnie informacji ABI w przypadku zaistnienia okoliczności:
   a) ustania zatrudnienia użytkownika u Administratora,
   b) zmiany zakresu obowiązków użytkownika.

7) Rozwiązanie umowy o pracę powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu, wykreślenie identyfikatora z ewidencji oraz unieważnienie jego hasła i identyfikatora.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1) Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
   a) przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwierania,
   b) sprawdzić stan okien i krat oraz ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych,
   c) sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek,
   d) po włączeniu komputera ocenić jakość jego pracy i stwierdzić ewentualne zmiany.

2) Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem. Po zalogowaniu się należy ocenić pracę systemu i stan zbioru danych.

3) Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:

   a) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób nieuprawnionych,
   b) dopilnować aby w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych, osoby trzecie przebywały tylko za zgodą przełożonych i w obecności osób uprawnionych,
   c) stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci elektrycznej. Potrzeby w tym zakresie zgłaszają ABI – przełożeni użytkownika,

4) Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
   a) wylogować się z systemu i zaczekać na jego wyłączenie się,
   b) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji,
   c) upewnić się, że szafy i biurka z dokumentacją są zamknięte,
   d) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie i klucze oddać w wyznaczone miejsce.

5) Po godzinach pracy Administrator lub osoba upoważniona przez niego zapewnia fizyczną ochronę pomieszczeń, w których przetwarzane są dane osobowe.

6) Pomieszczenia, w których przetwarzane są dane osobowe w zbiorach zarejestrowanych u Generalnego Inspektora Ochrony Danych Osobowych oraz zbiorach danych personalnych i finansowych – pracowników zatrudnionych przez Administratora, powinny być zabezpieczone, a klucze do nich deponowane po zakończonej pracy.

7) W przypadku stwierdzenia przez użytkownika prób niepowołanego naruszenia zabezpieczenia fizycznego pomieszczenia, zmian w systemie bezpieczeństwa systemu lub zauważenia, że stan urządzeń, zawartość zbiorów danych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie danych osobowych – postępuje zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy w Bierutowie."

Rozdział 5
Tworzenie i przechowywanie kopii awaryjnych.

1) Kopie awaryjne tworzy i przechowuje ASI, za pomocą odpowiednio skonfigurowanej aplikacji przeznaczonej do tego celu. Należy je wykonywać w każdy dzień roboczy. Kopie awaryjne należy tworzyć na odpowiedniej jakości nośnikach informacji, które należy szczegółowo opisać i przechowywać zgodnie z przepisami.

2) Kopiowanie danych osobowych na nośniki informacji oraz robienie wydruków jest zabronione chyba, że istnieje konieczność ich sporządzania, która wynika z nałożonych na użytkownika obowiązków i jest dozwolone przepisami prawa. Wykorzystywanie nośników informacji lub wydruków w innym celu jest zabronione.

3) Czas przechowywania codziennych kopii awaryjnych, jeżeli nie stanowią inaczej przepisy prawa, należy ograniczyć do 2 tygodni. Należy je przechowywać w innych pomieszczeniach niż zbiory danych osobowych. Kopie awaryjne przechowuje użytkownik w miejscach wskazanych przez przełożonego, zapewniających im odpowiednie warunki bezpieczeństwa.

4) Zdezaktualizowane i uszkodzone kopie awaryjne należy mechanicznie niszczyć w sposób uniemożliwiający ich ponowne użycie.

5) Nie wolno sporządzać wydruków z kopii awaryjnych i innych nośników informacji, które podlegają zniszczeniu.

Rozdział 6
Ochrona systemu informatycznego przed wirusami komputerowymi.

1) Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta powinna być zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji.

2) Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

3) Obowiązkiem ASI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego.

Rozdział 7
Przechowywanie nośników informacji, w tym kopii informatycznych i wydruków.

1) Nośniki informacji, w tym kopie informatyczne i wydruki komputerowe przechowuje się wyłącznie wówczas, gdy jest to konieczne i dozwolone przepisami prawa.

2) Nośniki informacji, w tym wydruki komputerowe przechowuje się w wyznaczonych pomieszczeniach w szafach i innych meblach biurowych, które posiadają odpowiednie zamknięcia, uniemożliwiające niepowołany dostęp do nich osób trzecich.

3) Pomieszczenia, o których mowa w pkt 2 winny spełniać określone warunki bezpieczeństwa, a w szczególności posiadać:
   a) wewnętrzne ściany, gwarantujące trwałe oddzielenie ich od innych pomieszczeń,
   b) pełne drzwi wejściowe, zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania,
   c) odpowiednie zabezpieczenie okien przed dostępem z zewnątrz i obserwacją,
   d) w razie uzasadnionej potrzeby ABI wprowadza dalej idące środki bezpieczeństwa dotyczące przechowywania nośników informacji w szafach i innych meblach biurowych, zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania, tj. w szczególności zamek patentowy lub szyfrowy.

Rozdział 8
Przeglądy i konserwacje systemów oraz zbiorów danych osobowych.

1) Okresowe przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu, wykonuje ASI lub osoba upoważniona przez Administratora Danych Osobowych.
2) Bieżącą konserwację i naprawę sprzętu może wykonywać inny pracownik, oprócz ASI posiadający stosowny zapis w zakresie czynności.

3) Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw w autoryzowanych firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych albo naprawia się je pod nadzorem ASI.

4) Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku, gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

5) Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do przekazania innemu podmiotowi, który nie jest uprawniony do otrzymania takich danych, należy wcześniej pozbawić zapisów danych.

Rozdział 9
Postępowanie w zakresie komunikacji w sieci komputerowej.

1) Komunikacja w sieci komputerowej jest dozwolona tylko po odpowiednim zalogowaniu się i podaniu indywidualnego hasła użytkownika. Uprawnienia wydaje ABI na pisemny wniosek przełożonego użytkownika.

2) Wprowadzanie do systemu informacji z zewnątrz jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i przez użytkownika posiadającego uprawnienia, wynikające z zakresu jego obowiązków.

3) Pomieszczenie, w którym znajdują się serwery systemów, są wydzielone wyłącznie dla potrzeb systemów informatycznych, posiadają wentylację wymuszoną oraz spełniają warunki zawarte w rozdziale 7 pkt 3. Dostęp do w/w pomieszczenia powinien mieć ABI, ASI oraz inny pracownik posiadający stosowny zapis w zakresie czynności, zastępujący ASI.

Rozdział 10
Postanowienia końcowe.

1) Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI lub inny pracownik posiadający stosowny zapis w zakresie czynności.

2) ASI prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych".

3) ASI lub wyznaczona przez ABI osoba realizuje „Program szkolenia użytkowników systemów informatycznych, w których przetwarzane są dane osobowe".

4) ASI dokonuje sprawdzenia sprawności funkcjonowania zabezpieczeń systemów, w których przetwarzane są dane osobowe, nie rzadziej niż raz na rok.

5) Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.

6) Nadużycie przez użytkownika postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.

7) W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926 ze zm.) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).