Zarządzenie Nr 176/2014
Wójta Gminy Michałowice
z dnia 25 sierpnia 2014 r.

w spranie wprowadzenia Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa danych osobowych.

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2013 r. poz. 594 ze zm.) oraz art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.), a także § 3 w związku z § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 Nr 100. poz. 1024) zarządzam, co następuje:

§ 1

Wprowadzam i wdrażam do stosowania Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Michałowice w brzmieniu stanowiącym załącznik Nr 1 do niniejszego zarządzenia oraz Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice w brzmieniu stanowiącym załącznik Nr 2 do niniejszego zarządzenia.

§ 2

Zobowiązuję wszystkich pracowników Urzędu Gminy Michałowice do zapoznania się z dokumentacją określona w § 1.

§ 3

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia określone w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz w Polityce bezpieczeństwa przetwarzania danych osobowych.

§4

Wykonanie zarządzenia powierza się Sekretarzowi Gminy Michałowice

§5

Traci moc Zarządzenie Nr 174/2009 Wójta Gminy Michałowice z dnia 14 września 2009r w sprawie wprowadzenia i wdrożenia do stosowania Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa danych osobowych.

§6

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY MICHAŁOWICE
mgr inż. Krzysztof Grabka

GŁÓWNY SPECJALISTA
ds. informatyki
inż. Marcin Walichnowski

RADCA PRAWNY
Joanna Domańska
WI-C-851

Załącznik nr 1
do Zarządzenia nr 176/2014
z dnia 25 sierpnia 2014 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY MICHAŁOWICE

ZATWIERDZAM
WÓJT GMINY MICHAŁOWICE
mgr inż. Krzysztof Grabka

(podpis Administratora Danych)

Opracował:

Marcin Walichnowski

GŁÓWNY SPECJALISTA
ds. informatyki
inż. Marcin Walichnowski

POSTANOWIENIA OGÓLNE

§ 1.

Polityka bezpieczeństwa, zwana dalej Polityką została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) zwanym dalej rozporządzeniem.

§ 2.

Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Urzędzie Gminy Michałowice

§ 3.

Ilekroć w Polityce jest mowa o :

1) **jednostce organizacyjnej, jednostce lub Urzedzie** - rozumie się przez to Urząd Gminy Michałowice;

2) **zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

4) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

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

6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji w celu przetwarzania danych osobowych na papierze;

7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

9) **Kierowniku jednostki** – rozumie się przez to Wójta Gminy Michałowice

10) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** -w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to kierownika jednostki który decyduje o celach i środkach przetwarzania danych osobowych;

11) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)** - rozumie się przez to osobę wyznaczoną przez kierownika jednostki, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

12) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę lub osoby zatrudnione przez kierownika jednostki upoważnione do realizacji zadań związanych z zarządzaniem systemem informatycznym;

13) **kierowniku komórki organizacyjnej** – pojęcie obejmuje również samodzielne stanowisko pracy,

14) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez kierownika jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który został zaznajomiony ze stosownymi przepisami prawa oraz dokumentami wewnętrznymi dotyczącymi ochrony tych danych;

15) **reprezentancie** - rozumie się przez to osobę uprawnioną do składania oświadczeń woli w imieniu Administratora Danych;

16) **zgodzie osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;

17) **ustawie** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.);

18) **Polityce** – rozumie się przez to niniejszy dokument;

19) **Instrukcji** – rozumie się przez to „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Michałowice" opracowaną na podstawie przepisów ustawy i rozporządzenia.

Rozdział I
CELE

§ 4.

Dane osobowe w Urzędzie są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych na dokumentach

papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 5.

Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:

1) **w formie papierowej** - przetwarzanej w ramach systemu tradycyjnego;

2) **w formie elektronicznej** - przetwarzanej w ramach systemu informatycznego.

§ 6.

Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.

§ 7.

Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Urzędu, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Urzędzie (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów).

§ 8.

Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w celach i na zasadach określonych w Rozdziale 3 (Art. 23-31a) ustawy

§ 9.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują kierownicy komórek organizacyjnych.

§ 10.

1. Z zasadami w Polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, potwierdzają to składając odpowiednie oświadczenie, którego wzór stanowi załącznik nr 1 do niniejszej Polityki.

2. Oświadczenia przechowywane są w aktach osobowych pracownika.

§ 11.

1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych posiadają dostęp jedynie osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik nr 2 do niniejszej polityki.

2. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla poszczególnych komórek organizacyjnych Urzędu.

3. Upoważnienia określone w ust. 1 przechowywane są w aktach osobowych pracownika.

4. Ewidencję osób biorących udział w przetwarzaniu danych osobowych prowadzi stanowisko do spraw kadr.

5. Wzór ewidencji określonej w ust. 4 stanowi załącznik nr 3 do Polityki bezpieczeństwa.

§ 12.

1. Wnioski o nadanie stosownych uprawnień do przetwarzania danych osobowych przedkładają kierownicy komórek organizacyjnych lub osoby obejmujące samodzielne stanowiska Administratorowi Bezpieczeństwa Danych, za pośrednictwem stanowiska do spraw kadr.

2. Wnioski o których mowa w ust. 1 zawierają listę zbiorów danych osobowych do których dostęp jest niezbędny pracownikowi zgodnie z jego zakresem obowiązków

3. Wzór wniosku stanowi załącznik nr 4 do Polityki

§ 13.

1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w Urzędzie dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione środkami technicznymi adekwatnymi do kategorii danych oraz występujących zagrożeń.

Rozdział II
ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 14.

1. Za bezpieczeństwo i organizację przetwarzania danych osobowych odpowiada Administrator Danych Osobowych.

2. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 15.

Administrator Danych Osobowych może wyznaczyć Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 16.

1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi.
2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych.
3. Administrator Bezpieczeństwa Informacji posiada wgląd do ewidencj osób upoważnionych do przetwarzania danych osobowych.
4. Do zakresu odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji należy:
   1) nadzór nad bezpieczeństwem systemów informatycznych;
   2) nadzór nad przestrzeganiem przez wszystkich użytkowników stosowania obowiązujących procedur;
   3) weryfikacja ewidencji o której mowa § 11 ust. 4 oraz kont dostępowych kont użytkowników systemu informatycznego;
   4) doradztwo użytkownikom w zakresie bezpieczeństwa;
   5) dbanie, aby dostęp do systemu posiadali użytkownicy mający stosowne zezwolenia oraz przeszkoleni w zakresie stosowania obowiązujących procedur bezpieczeństwa;
   6) prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych,

§ 17.

1. Administrator Danych Osobowych wyznacza Administratorów Systemu Informatycznego, którzy posiadają najwyższe uprawnienia w systemie informatycznym. Tylko ASI są osobami uprawnionymi do instalowania i usuwania oprogramowania systemowego oraz narzędziowego.
2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.
3. Do zakresu odpowiedzialności i obowiązków Administratora Systemu Informatycznego należy:
   1) zapewnianie stałej sprawności urządzeń mających wpływ na bezpieczeństwo danych;
   2) odpowiadanie za bezpieczeństwo systemu informatycznego;
   3) zobowiązywanie i bieżąca kontrola stosowania się użytkowników do obowiązujących procedur;
   4) utrzymywanie i aktualizowanie kont użytkowników systemu informatycznego;

5) zapewnianie aktualizacji dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności;

6) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;

7) wykonywanie kopii awaryjnych/archiwalnych oraz nadzór nad ich przechowywaniem;

8) wprowadzanie i nadzór nad mechanizmami autoryzacji.

§ 18.

Kierownik komórki organizacyjnej odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników, ze szczególnym uwzględnieniem zbiorów tradycyjnych (papierowych);

2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie;

3) zgłasza ABI planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie, wzór wniosku stanowi załącznik nr 5 do Polityki;

4) wnioskuje do Kierownika Jednostki o nadanie upoważnień do przetwarzania danych osobowych pracownikom, wzór wniosku stanowi załącznik nr 2 do Polityki;

5) wnioskuje do ASI o przyznanie dostępu do zbiorów danych zgromadzonych w systemie informatycznym, wzór wniosku stanowi załącznik nr 4 do Polityki;

6) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Urzędzie;

§ 19.

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem komputerowej stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za implementację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

Rozdział III
WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§ 20.

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej, w postaci dokumentów papierowych oraz w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik nr 6 do polityki bezpieczeństwa.

§ 21.

Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Urzędzie wyróżnia się dwie kategorie danych:

1) dane osobowe zwykłe - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych;

2) dane osobowe wrażliwe - zgodnie z katalogiem zawartym w treści ustawy o ochronie danych osobowych (art. 27 ust. 1) wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 22.

Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na rodzaj gromadzonych danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 tejże ustawy.

Rozdział IV
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 23.

1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.

3. Bezwzględnie zabronione jest podłączanie urządzeń (w szczególności komputerów) innych niż służbowe do sieci wewnętrznej Urzędu bez zgody i wiedzy ASI

4. Bezwzględnie zabronione jest podłączanie do komputerów w sieci wewnętrznej urządzeń (takich jak modemy GPRS, 3G, LTE itp.) nawiązujących połączenia do sieci

zewnętrznych (np. Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi, WiMAX itp.).

§ 24.

Systemy dziedzinowe, przetwarzające dane osobowe mogą wymieniać się zgromadzonymi danymi, z zachowaniem zasad przetwarzania danych opisanych w ustawie, sposób połączeń i przepływu danych opisuje załącznik nr 7

Rozdział V
OKREŚLENIE ŚRODKÓW TECHNICZNYCH i ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 25.

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administratorzy Systemu Informatycznego zapewniający jego prawidłową eksploatację.
2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.
3. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.
4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Rozdział VI
UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 26.

1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:
   1) jakie dane osobowe zawiera zbiór;
   2) w jaki sposób zebrano dane;
   3) w jakim celu i zakresie dane są przetwarzane;
   4) w jakim zakresie oraz komu dane zostały udostępnione.

chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek, o wystąpieniu osoby której dane dotyczą, poinformować administratora danych.

§ 29.

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.

2. Administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 30.

Powierzenie przetwarzania danych osobowych (to jest wglądu, modyfikacji lub usuwania zgromadzonych danych) innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez Administratora Danych Osobowych.

Rozdział VII
ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 31.

Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.

§ 32.

1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

2. Hasło użytkownika podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział VIII
BEZPIECZEŃSTWO FIZYCZNE

§ 33.

1. Dane osobowe, które są przedmiotem zainteresowania ustawy o ochronie danych osobowych, gromadzone i przechowywane są w systemie komputerowym oraz w postaci akt.

2. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 34.

1. Obszar przetwarzania danych osobowych w Urzędzie obejmuje pomieszczenia wymienione w załączniku nr 8 do Polityki.
2. Przetwarzanie danych poza obszarem określonym w ust. 1 jest zabronione.
3. Przenoszenie wydruków komputerowych oraz akt pomiędzy pomieszczeniami wymienionymi w załączniku nr 8 należy wykonywać w sposób uniemożliwiający wgląd do dokumentów.
4. Surowo zabronione jest pozostawianie jakichkolwiek wydruków w pomieszczeniach ogólnodostępnych bez nadzoru (np. „*ksero*", korytarze, pomieszczenia socjalne), niedopełnienie tego obowiązku uważa się za ciężkie naruszenie obowiązków pracowniczych.

§ 35.

Pomieszczenia, w których znajdują się akta lub systemy służące do przetwarzania danych osobowych winny być:

1) wyposażone w szafy zamykane na klucz umożliwiające przechowywanie dokumentów, w sposób zabezpieczający przed dostępem osób nieposiadających stosownych upoważnień,
2) zamknięte, jeśli nikt w nich nie przebywa.

§ 36.

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą kierownika komórki organizacyjnej, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

Dział IX
BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 37.

Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

§ 38.

Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy i zgody kierownika komórki organizacyjnej oraz ASI.

§ 39.

Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 40.

1. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.
2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.
3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana (podejrzenie ujawnienia hasła), osoba przetwarzającej dane powinna niezwłocznie dokonać zmiany hasła.
4. Komputery za pomocą których uzyskiwany jest dostęp do zbiorów danych osobowych chronione są osobnym hasłem.
5. W przypadku opuszczenia stanowiska pracy użytkownik ma obowiązek zabezpieczyć stanowisko komputerowe przed dostępem (uruchomić wygaszacz ekranu lub wylogować się z systemu).
6. Użytkownik ma obowiązek zmiany haseł nie rzadziej niż co 30 dni, szczegółowe zasady tworzenia haseł określa Instrukcja.

§ 41.

1. Elektroniczne bazy danych osobowych są archiwizowane.
2. Kopie są wykonywane na nośnikach danych lub w magazynach dyskowych do tego przeznaczonych.
3. Szczegółowe zasady tworzenia kopii zapasowych określa Instrukcja.

§ 42.

Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie oprogramowanie niezbędne do wykonywania wyznaczonego zakresu obowiązków.

Rozdział X
KONSERWACJE I NAPRAWY

§ 43.

Każde urządzenie użytkowane w systemie informatycznym., powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

§ 44.

Za konserwację oprogramowania systemowego oraz aplikacyjnego systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.

§ 45.

Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

1) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w szafie metalowej znajdującej się w strefie o ograniczonym dostępie lub w sejfie do którego dostęp ma Kierownik jednostki oraz ASI;

2) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

Dział XI
PLANY AWARYJNE I ZAPOBIEGAWCZE

§ 46.

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), znacząco obniży ryzyko awarii systemu w przypadku awarii zasilania.

§ 47.

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, automatycznej archiwizacji oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na tydzień. Kopie archiwalne danych są wykonywane na nośnikach danych lub w magazynach dyskowych. Użycie kopii zapasowych następuje w przypadku odtwarzania systemu po awarii.

§ 48.

Administrator Systemu Informatycznego okresowo kontroluje poprawność kopii zapasowych oraz przydatność do odtworzenia systemu po awarii.

§ 49.

W przypadku wykrycia problemów z odtworzeniem danych z kopi zapasowej ASI niezwłocznie zawiadamia ABI o wykrytym problemie w celu opracowania nowych procedur wykonywania kopii zapasowych, uwzględniających rozwiązanie wykrytego problemu.

Rozdział XII
POLITYKA ANTYWIRUSOWA

§ 50.

1. Wszystkie komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

1) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;

2) zabrania się instalowania oprogramowania typu „freeware" lub „shareware" oraz nieznanego pochodzenia bez zgody i wiedzy Administratora Systemu Informatycznego;

3) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

3. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z Administratorem Systemu Informatycznego.

Rozdział XIII
PRZEPISY KOŃCOWE

§ 51.

Celowe lub nieumyślne naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy art.49-54a tj: grzywnie, karze ograniczenia wolności albo pozbawienia wolności od roku do lat trzech w zależności od wagi naruszenia

§ 52.

W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy oraz 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)

§ 53.

Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Jednostce, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

§ 54.

Niniejszy dokument jest dokumentem wewnętrznym i nie może być udostępniany osobom postronnym w żadnej formie.

Załącznik nr 1
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice”*

Reguły, dnia ……
(miejscowość, data)

_____
(imię i nazwisko)

OŚWIADCZENIE

Oświadczam, iż zostałem(am) zaznajomiony(a) z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. z 2002 r. Dz. U. Nr 101, poz. 926 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych *„Polityką bezpieczeństwa przetwarzania danych osobowych”* oraz *„Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”*.

Jednocześnie zobowiązuję się do ich przestrzegania.

(podpis osoby składającej oświadczenie)

Załącznik nr 2
do *„Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice”*

_____
(imię i nazwisko)

Reguły, dnia ……
(miejscowość, data)

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. z 2002 r. Dz. U. Nr 101, poz. 926 ze zm.), upoważniam Pana/Panią do przetwarzania danych osobowych.

Upoważnienie obejmuje prawo wglądu, wprowadzania, modyfikowania i usuwania danych osobowych. [1)]

Zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych *„Polityki bezpieczeństwa przetwarzania danych osobowych”* oraz *„Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”*.

_____
(podpis Administratora Danych)

1) *Niepotrzebne skreślić*