Załącznik Nr 2 do zarządzenia
Wójta Gminy Męcinka
z dnia 4 lipca 2012 roku

Instrukcja przetwarzania danych osobowych

Rozdział I
Postanowienia ogólne

§ 1.

Przez użyte w Instrukcji określenia, należy rozmieć:

1/ ustawa – ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zmianami),

2/ administrator danych – pracownik Urzędu Gminy Męcinka, właściwy do załatwienia spraw w zakresie ochrony danych osobowych z wyłączeniem spraw zastrzeżonych w niniejszym zarządzeniu dla Wójta Gminy Męcinka; właściwego pracownika ustala się na podstawie regulaminu organizacyjnego Urzędu Gminy Męcinka nadawanego przez Wójta Gminy Męcinka w drodze zarządzenia,

3/ administrator bezpieczeństwa informacji – pracownik Urzędu Gminy Męcinka lub inna osoba wyznaczona do nadzorowania przestrzegania zasad ochrony określonych w niniejszej instrukcji oraz wymagań wynikających z przepisów szczególnych o ochronie danych osobowych,w tym również administratora danych osobowych,

4/ urząd – Urząd Gminy Męcinka,

5/ pracownik – osoba zatrudniona w ramach stosunku pracy w urzędzie i upoważniona do przetwarzania danych osobowych w systemie informatycznym,

6/ sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jego potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

7/ wójta gminy – Wójta Gminy Męcinka,

8/ kierownika komórki organizacyjnej – należy przez to rozumieć sekretarza gminy, skarbnika gminy, kierownika referatu,

9/ polityka bezpieczeństwa – polityka bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy Męcinka.

§ 2.

Do administratora danych należy prowadzenie całokształtu spraw związanych z przetwarzaniem danych osobowych, a w szczególności:

1) udostępnianie danych osobowych,
2) kontrola i nadzór w zakresie przestrzegania zasad i procedur przetwarzania danych osobowych w urzędzie, z uwzględnieniem kryterium celowości i adekwatności oraz warunków organizacyjno – technicznych,
3) rejestracja zbiorów danych osobowych w rejestrze Generalnego Inspektora Ochrony Danych Osobowych,
4) prowadzenie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych,
5) przygotowywanie umowy o powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu oraz kontrolę przestrzegania jej postanowień po podpisaniu przez wójta gminy.

§ 3.

1. Administrator bezpieczeństwa informacji, w szczególności:
   1) zarządza i nadzoruje systemem informatycznym, gdzie przetwarzane są dane osobowe,
   2) ponosi odpowiedzialność za bezpieczeństwo danych osobowych i zbiorów danych osobowych w systemie informatycznym,
   3) podejmuje działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego.
2. Kierownik komórki organizacyjnej wykonuje czynności przetwarzania danych osobowych w ramach zbiorów, funkcjonujących na nadzorowanym stanowisku, z upoważnienia administratora danych, z możliwością udostępniania danych osobowych na zasadach przewidzianych w § 6.
3. Pracownik przetwarza dane osobowe z upoważnienia administratora danych, w zakresie obowiązków pracowniczych bądź czynności wskazanych w umowie, z wyłączeniem czynności udostępniania danych osobowych.
4. W przypadku wykonywania zadań,których mowa w ust.1 przez administratora danych,współpracuje on z podmiotem zewnętrznym,któremu zlecono obsługę informatyczną w urzędzie.

Rozdział II
Obowiązki pracowników

§ 4.

1. Obowiązek ochrony danych osobowych dotyczy wszystkich pracowników, którzy mają do nich dostęp.
2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nieupoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.

§ 5.

1. Osoby wymienione w § 3, są zobowiązane do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
2) stosowania określonych przez administratora danych zasad, procedur oraz wytycznych mających na celu właściwe adekwatne przetwarzanie danych,
3) należytego zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,
4) zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony interesu osób, których dane dotyczą.

2. Kierownik komórki organizacyjnej, poza obowiązkami wymienionymi w ust. 1, jest zobowiązany do:
1) zapewnienia organizacyjno - technicznej ochrony danych osobowych,
2) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych osobowych przez podległych pracowników,
3) sygnalizowanie niezgodności aktów prawnych gminy oraz innych aktów wewnętrznych urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawiania stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej,
4) zwracanie się do administratora danych, w przypadku wątpliwości co do stosowania przepisów prawnych z zakresu ochrony danych osobowych, o wiążące wytyczne.

Rozdział III
Procedury szczegółowe

§ 6.

1. Administrator danych może upoważnić do dostępu i nadać uprawnienia do udostępnienia danych osobowych w zakresie szczegółowo określonych zbiorów urzędu:
   1) kierownika komórki organizacyjnej – z własnej inicjatywy,
   2) pozostałych pracowników – na wniosek kierownika komórki organizacyjnej.
2. W okolicznościach zmiany zakresu obowiązków bądź stanowiska lub funkcji, administrator danych cofa upoważnienia, o którym mowa w ust. 1 na uzasadniony wniosek, o którym mowa w ust. 1 pkt 2.
3. Wzór upoważnienia, o którym mowa w ust. 1 stanowi załącznik nr 1 do niniejszej Instrukcji.

§ 7.

1. W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, właściwy kierownik komórki organizacyjnej zobowiązany jest zwrócić się do administratora danych o wydanie upoważnienia do przetwarzania danych osobowych, którego wzór stanowi załącznik nr 2 do niniejszej Instrukcji.
2. Pracownik, o którym mowa w ust. 1, któremu udzielono stosownego upoważnienia według wzoru ustalonego załącznikiem nr 1 do niniejszej Instrukcji, jest zobowiązany do podpisania oświadczenia, którego wzór stanowi załącznik nr 3 do niniejszej Instrukcji.
3. W przypadku zmiany stanowiska bądź zakresu obowiązków pracowniczych, kierownik komórki organizacyjnej jest zobowiązany bezzwłocznie skierować wniosek o wydanie bądź cofnięcie stosownego upoważnienia, którego wzór stanowi załącznik nr 2 do niniejszej Instrukcji.

§ 8.

1. W przypadku nawiązania stosunku pracy na stanowisku kierownika komórki organizacyjnej, w zakresie którego jest prowadzenie zbiorów danych osobowych, administrator danych wyda upoważnienie do przetwarzania danych osobowych.
2. W przypadku zmiany na stanowisku kierownika komórki organizacyjnej administrator danych cofa upoważnienie do przetwarzania danych osobowych.

§ 9.

1. Rozwiązanie stosunku pracy powoduje wygaśnięcie upoważnienia.
2. Wypowiedzenie umowy o pracę przez wójta gminy lub pracownika powoduje wygaśnięcie upoważnienia do przetwarzania danych, o którym mowa w § 7, z dniem wręczenia wypowiedzenia umowy o pracę.

§ 10.

1. Administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych, o których mowa w § 3.
2. Administrator bezpieczeństwa informacji współpracuje z administratorem danych w zakresie aktualizacji ewidencji, o której mowa w ust. 1, a dotyczącej identyfikatorów pracowników, którzy posiadają upoważnienia, o których mowa w § 3.Postanowienia § 3 ust.4 stosuje się odpowiednio.

§ 11.

1. W przypadku konieczności utworzenia nowego zbioru danych, wynikającej z obowiązków nałożonych przepisami ustawy bądź nowymi zadaniami, kierownik komórki organizacyjnej lub pracownik zobowiązany jest niezwłocznie – nie później jednak niż w ciągu 30 dni od dnia powstania obowiązku utworzenia zbioru – złożyć administratorowi danych projekt wniosku o zatwierdzenie zbioru danych osobowych w celu zgłoszenia danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.
2. Postanowienia ust. 1 stosuje się odpowiednio do zmian informacji objętych zgłoszonym zbiorem.

§ 12.

1. W obiegu zewnętrznym dane osobowe udostępnia ze zbiorów administrator danych lub osoba, o której mowa w § 3 ust. 2.
2. W obiegu wewnętrznym między stanowiskami pracy urzędu można udostępniać dane osobowe, jeśli przepisy szczególne zabraniają tego w następującym trybie: informacje zawierające imię i nazwisko, adres zamieszkania i inne o charakterze podstawowym, bezpośrednio identyfikujące osobę fizyczną może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej".

3. Tryb, określony w ust. 2 może być w uzasadnionych przypadkach stosowany również w wymianie informacji i danych osobowych między stanowiskiem pracy urzędu a jednostką organizacyjną gminy.
4. Przekazywanie danych w trybie ust. 2 i 3 może odbywać się tylko i wyłącznie w przypadku toczącego się postępowania administracyjnego bądź cywilnego w stosunku do osoby, której dane dotyczą.

Rozdział IV
Zarządzanie systemem informatycznym służącym przetwarzaniu danych osobowych

§ 13.

Uwzględniając kategorie danych osobowych oraz stopień bezpieczeństwa ich przetwarzania w systemie informatycznym, wprowadza się w urzędzie poziom wysoki.

§ 14.

W urzędzie obowiązują następujące procedury nadawania i zmiany uprawnień do przetwarzania danych:

1) każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z przepisami regulującymi ochronę danych osobowych, polityką bezpieczeństwa oraz niniejszą Instrukcją,
2) zapoznanie się z dokumentami, o których mowa w pkt 1 pracownik potwierdza własnoręcznym podpisem,
3) administrator danych przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego wniosku kierownika komórki organizacyjnej lub z własnej inicjatywy, określającego zakres uprawnień pracownika,
4) jedynie prawidłowo wypełniony wniosek o nadanie uprawnień w systemie oraz zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie,
5) przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji,
6) hasło ustanowione podczas przyznawania uprawnień należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym,
7) pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony,
8) pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu,
9) wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych,
10) w systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji,
11) identyfikator użytkownika w aplikacji powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej,
12) odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika komórki organizacyjnej, któremu pracownik podlega lub z inicjatywy administratora danych, z podaniem daty oraz przyczyny odebrania uprawnień,

13/) kierownicy komórek organizacyjnych zobowiązani są pisemnie informować administratora danych o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym,
14) identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło,
15) administrator danych, zobowiązany jest do prowadzenia ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym,
16/)rejestr, którego wzór stanowi załącznik nr 4, powinien zawierać:
   a) imię i nazwisko użytkownika systemów informatycznych,
   b) rodzaj uprawnienia,
   c) datę nadania uprawnienia,
   d) datę odebrania uprawnienia,
   e) przyczynę odebrania uprawnienia,
   f) podpis administratora bezpieczeństwa informacji,
17) rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

§ 15.

Przetwarzanie danych osobowych musi być zorganizowane poprzez system haseł i zgodnie z następującymi zasadami:
1) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła,
2)hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu,
3) identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie,
4) pracownicy są odpowiedzialni za zachowanie poufności swoich haseł,
5)hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności,
6) pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone,
7) hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie,
8) w sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła,
9)przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła – 6 znaków,
   b) zakazuje się stosować:
      - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
      - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
      - swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
      - imion (w szczególności imion osób z najbliższej rodziny),
      - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.,
      - wyrazów słownikowych,

- przewidywalnych sekwencji znaków z klawiatury, np. „QWERTYUI”,”12345678”, itp.,

c) należy stosować:
- hasła zawierające małe i duże litery,
- hasła zawierające kombinacje liter i cyfr,
- hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole: @, #, &, itp.,
- hasła, które można zapamiętać bez zapisywania,
- hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

10) zmiany hasła nie wolno zlecać innym osobom,
11) w systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła, nie należy korzystać z tego ułatwienia.

§ 16.

W urzędzie obowiązują następujące procedury rozpoczęcia, zawieszania i zakończenia pracy w systemie:

1) przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła,
2)przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania z systemu (zablokowanie dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu,
3) osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu,
4) przed wyłączeniem komputera należy bezwzględnie zakończyć pracę programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować z sieci komputerowej,
5) niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

§ 17.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada administrator danych w porozumieniu z podmiotem zewnętrznym, któremu zlecono obsługę informatyczną urzędu a w przypadku nieobecności administratora inny pracownik wskazany przez wójta gminy.

2. Kopie bezpieczeństwa wykonywane są zgodnie z § 5 ust. 2 pkt 6 polityki bezpieczeństwa po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
3. Płyty CD-R przechowuje się w metalowej szafie w pok.Nr 18.

4. W przypadku wykonywania zabezpieczeń długoterminowych na dyskietkach lub płytach CD-R, nośniki te należy co kwartał sprawdzać pod kątem ich dalszej przydatności.

§ 18.

Praca z użyciem elektronicznych nośników informacji odbywa się wyłącznie po spełnieniu następujących warunków:

1) dane osobowe w postaci elektronicznej, zapisane na dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę urzędu.

2) wymienne elektroniczne nośniki informacji są przechowywane w biurach stanowiących obszar przetwarzania danych osobowych, określony w polityce bezpieczeństwa,

3) po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach,

4) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

5) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych,

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

7) kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w odrębnym sejfie urzędu,

8/) dostęp do miejsca przechowywania mają tylko upoważnieni pracownicy.

§ 19.

Ustala się następujące zasady wykonywania i przechowywania wydruków, zawierających dane osobowe:

1) w przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom nieupoważnionym,
2) pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy,
3) wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 20.

W celu ochrony systemów podejmuje się następujące działania:

1) na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora,

2) każdy e-mail wpływający do urzędu musi być sprawdzany pod kątem występowania wirusów przez bramę antywirusową,
3) definicje wzorów wirusów aktualizowane są nie rzadziej niż raz w miesiącu,
4) zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym; sprawdzenia dokonuje pracownik, który nośnik zamierza użyć,
5) zabrania się pobierania z internetu plików niewiadomego pochodzenia; każdy plik pobrany z internetu musi być sprawdzony programem antywirusowym; sprawdzenia dokonuje pracownik, który pobrał plik,
6) zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym; sprawdzenia dokonuje pracownik, który pocztę otrzymał,
7) kontrola antywirusowa przeprowadzona jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania,
8) w przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

§ 21.

Odnotowywanie w systemie informacji o udostępnieniu danych odbywa się przy zastosowaniu następujących zasad:

1) dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym,
2) udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga zgody wójta gminy lub osoby przez niego upoważnionej,
3) udostępnienie danych osobowych „na zewnątrz" nie może być realizowane drogą telefoniczną, z zastrzeżeniem § 12 ust. 2,
4) udostępnienie danych osobowych może nastąpić wyłącznie zgodnie z art. 29 ust. 3 ustawy,

§ 22.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić administratora bezpieczeństwa informacji.

3. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

4. Administrator danych w porozumieniu z podmiotem prowadzącym obsługę informatyczną urzędu zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.

5. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R.

§ 23.

Połączenie lokalnej sieci komputerowej urzędu z internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych (firewall,proxy) oraz kompleksowego oprogramowania antywirusowego.

§ 24.

1. Komputery przenośne, mogą być zakupione wyłącznie dla pracowników urzędu i przekazane do użytkowania po podpisaniu protokołu odbioru.
2. Komputery przenośne muszą posiadać zabezpieczenia techniczne, celem których jest poufność danych osobowych, jednak zabronione jest tworzenie na nich i przetwarzanie zbiorów danych osobowych.
3. Ewidencję przenośnego sprzętu informatycznego prowadzi sekretarz gminy.

Rozdział V
Postępowanie w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego

§ 25.

Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:
1/)stanu urządzeń technicznych,
2) zawartości zbiorów danych osobowych,
3) sposobu działania programu lub jakości komunikacji w sieci telefonicznej,
4) metod pracy (w tym obiegu dokumentów).

§ 26.

W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:
1) powiadomić administratora danych, bezpośredniego przełożonego lub wójta gminy,
2) zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych,
3) podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia – o ile czynności te nie spowodują przekroczenia uprawnień pracownika,
4) zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.

§ 27.

1. Bezpośredni przełożony pracownika po otrzymaniu powiadomienia o naruszeniu bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić administratora danych lub wójta gminy, chyba, że zrobił to pracownik, który stwierdził naruszenie.
2. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych administrator danych i przełożony pracownika przejmują nadzór nad pracą w systemie odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu podjęcia stosownej decyzji.

§ 28.

Administrator danych, a w przypadku jego nieobecności osoba upoważniona przez wójta gminy, podejmuje czynności wyjaśniające mające na celu ustalenie:
1) przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych,
2) osób winnych naruszenia bezpieczeństwa danych osobowych,
3)skutków naruszenia.

§ 29.

1. Administrator danych zobowiązany jest do powiadomienia o zaistniałej sytuacji wójta gminy, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.
2. Administrator danych w porozumieniu z podmiotem któremu zlecono obsługę informatyczną urzędu zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego, co najmniej:
   1) datę i miejsce wystąpienia naruszenia,
   2) zakres ujawnionych danych,
   3) przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy,
   4) sposób rozwiązania problemu,
   5) przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Raport ten administrator danych przekazuje wójtowi gminy lub upoważnionej przez niego osobie.

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zmianami),

u p o w a ż n i a m

Pana/ią .....

zatrudnioną/nego w .....

na stanowisku.....

do wykonania czynności przetwarzania danych osobowych, z wyłączeniem udostępniania danych, w ramach zbiorów funkcjonujących na zajmowanym stanowisku zgodnie z zakresem przydzielonych obowiązków pracowniczych.

Męcinka, dnia.....

.....
Administrator Danych Osobowych

WNIOSEK

W związku z: */

a/ zatrudnieniem/zmianą stanowiska .....

b/ zmianą zakresu obowiązków pracowniczych.....

c/ utworzeniem nowego zbioru danych osobowych .....

d/ naruszeniem zasad i sposobu przetwarzania danych osobowych.....
.....

*/ *właściwe zakreślić i wypełnić*

W N I O S K U J Ę

o wydanie upoważnienia / o cofnięcie upoważnienia z dnia ..... */

dla Pani / Pana .....

zatrudnionej/nego w.....

na stanowisku .....

do wykonania czynności przetwarzania danych osobowych, z wyłączeniem udostępniania danych, w ramach zbiorów funkcjonujących na zajmowanym stanowisku zgodnie z zakresem przydzielonych obowiązków pracowniczych.

*/ *niewłaściwe skreślić*

Męcinka, dnia .....

OŚWIADCZENIE

Oświadczam, iż zapoznałem się z:

1) ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, z późn. zmianami).
2) Polityką Bezpieczeństwa Przetwarzania Danych Osobowych w systemie Informatycznym Urzędu Gminy Męcinka.
3) Instrukcją Zarządzania Systemem Informatycznym Urzędu Gminy Męcinka.

i zobowiązuję się do przestrzegania tajemnicy ochrony danych osobowych, a w szczególności:

- zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą, w trakcie trwania stosunku pracy,
- zabezpieczania danych przed ich udostępnieniem osobom nieupoważnionym.

....

(data) (podpis pracownika)

REJESTR UŻYTKOWNIKÓW I UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

KARTA EWIDENCJI UPRAWNIEŃ OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH.

Identyfikator użytkownika	*Nazwisko i imię*

Lp.	Zakres upoważnienia	Data nadania uprawnień	Podpis osoby upoważnionej	Data i przyczyna odebrania uprawnień
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				