Załącznik Nr 1 do Zarządzenia Nr 20/2008 Wójta Gminy Miłkowice z dnia 2 kwietnia 2008r. w sprawie wprowadzenia do użytku służbowego „Instrukcji zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy Miłkowice" a także wprowadzenia do użytku służbowego „Polityki bezpieczeństwa przetwarzania danych osobowych"

Instrukcja

zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy Miłkowice

Spis treści

Rozdział 1.
Postanowienia ogólne

§ 1

Niniejsza Instrukcja określa sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych, oraz postępowania w sytuacjach naruszenia ochrony danych osobowych w Urzędzie Gminy Miłkowice. Zwana jest dalej **Instrukcją.** Jest dokumentem wewnętrznym wydanym przez Administratora Danych Osobowych - Wójta Gminy Miłkowice i ma zastosowanie do przetwarzania danych osobowych w systemach informatycznych urzędu w celu bezpiecznego ich wykorzystywania.

§ 2

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych Osobowych, zakres działania Administratora Bezpieczeństwa Informacji oraz wszystkich użytkowników, przetwarzających dane osobowe w systemach informatycznych Urzędu.

2. 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, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Z 2004 r. Nr 100, poz. 1024).

§ 3

Użyte w Instrukcji określenia i skróty oznaczają:

1) ***Jednostka*** – Urząd Gminy,

2) **Administrator Danych Osobowych** – Wójt Gminy Miłkowice – zwany dalej ***Administratorem.***

3) **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Administratora, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach – zwany dalej ***ABI.***

4) **Administrator Systemów Informatycznych i Sieci Informatycznej –** osoba wyznaczona przez Administratora, odpowiedzialna za sprawność i konserwację oraz wdrażanie techniczne zabezpieczeń systemów informatycznych oraz techniczne bezpieczeństwo przetwarzania danych w sieci informatycznej – zwana dalej ***ASI***.

5) **Osoba upoważniona lub użytkownik systemu -** osoba upoważniona przez Administratora i dopuszczona, w zakresie wskazanym w upoważnieniu, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym na danych przez samodzielne stanowiska pracy oraz wieloosobowe stanowiska pracy – zwana dalej ***użytkownikiem.***

6) **Osoba trzecia –** 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 i podejmująca czynności w zakresie **przekraczającym** ramy jego upoważnienia.

7) **System informatyczny -** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych – zwany dalej ***systemem.***

8) **Zabezpieczenie systemu** – wdrożenie przez Administratora odpowiednich środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.

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

10) **Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych** – zwana dalej ***ewidencją*** – prowadzona przez Administratora Bezpieczeństwa Informacji, zawierająca dane użytkowników upoważnionych do przetwarzania danych osobowych w zakresie ich danych osobowych, identyfikatorów, haseł, upoważnień.

11) **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

12) **Rozporządzenie** – rozporządzenie 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).

Rozdział 2.
Zabezpieczenie obszaru przetwarzania danych osobowych

§ 4

1. Obszar o którym mowa w Rozdziale **4 § 5** „Polityki bezpieczeństwa przetwarzania danych osobowych”, zabezpiecza się przed dostępem osób trzecich na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2. Przebywanie osób trzecich w obszarze, o którym mowa w Rodziale **4 § 5** „Polityki bezpieczeństwa przetwarzania danych osobowych”, jest dopuszczalna za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

Rozdział 3.
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

§ 5

Uprawnienia do przetwarzania danych osobowych nadawane są za zgodą Administratora danych lub na wniosek osoby przez niego upoważnionej. Uprawnienia dotyczą zarówno danych osobowych gromadzonych w systemie, jak i również w tradycyjnych rejestrach papierowych.

§ 6

1. Identyfikator służy do „logowania" się użytkownika w systemie.

2. **Identyfikator** jest to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

3. **Hasło** jest to ciąg znaków literowych, cyfrowych lub innych znany jedynie osobie upoważnionej do pracy w systemie informatycznym.

4. Każdy system w którym przetwarza się dane osobowe w zbiorach jednostki musi być wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do danych w postaci identyfikatorów i haseł.

5. Dla poszczególnych użytkowników Identyfikatory przydziela ABI. Ten sam identyfikator nie może być przydzielone innemu użytkownikowi.

§ 7

Funkcje Administratorem Bezpieczeństwa Informacji pełni informatyk zatrudniony w Urzędzie Gminy Miłkowice.

§ 8

Wprowadza się rejestr osób zatrudnionych przy przetwarzaniu danych osobowych oraz osób pracujących w systemie. Rejestr prowadzony jest przez Administratora Bezpieczeństwa Informacji w postaci elektronicznej i papierowej. W rejestrze dokonywane są wpisy dotyczące uprawnień dostępu do baz posiadających dane osobowe prowadzonych zarówno w systemie informatycznym jak również w tradycyjnych rejestrach papierowych.

§ 9

1. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu Identyfikatora i hasła, którymi się posługuje lub posługiwał.
2. 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 4.
Rejestrowanie i wyrejestrowywanie użytkowników, nadawanie uprawnień do korzystania z systemów.

§ 10

1. Rejestracji i wyrejestrowania użytkowników z systemu dokonuje ABI na polecenie Administratora, wprowadzając dane do ewidencji, o której mowa w § 8 niniejszej instrukcji.

2. Ewidencja musi zawierać:
    1) imię i nazwisko użytkownika,
    2) stanowisko służbowe użytkownika,
    3) czas trwania upoważnienia,
    4) datę zarejestrowania i wyrejestrowania z systemu,

5) zasoby elektroniczne jak i papierowe do których przetwarzania użytkownik jest upoważniony,
6) identyfikator jeśli upoważnienie dotyczy zasobu elektronicznego.

3. Jakakolwiek zmiana informacji określonych w ust. 2 podlega natychmiastowemu odnotowaniu w ewidencji

§ 11

1. Zarejestrowanie użytkownika w systemie odbywa się zgodnie z poniższymi procedurami:

1) złożenie wniosku przez użytkownika do ABI o udzielenie dostępu do przetwarzania danych osobowych – wzór załącznik **nr 1** do niniejszej instrukcji. wniosek musi być zatwierdzony przez Administratora,
2) podpisanie przez użytkownika ubiegającego się o dostęp do danych, oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych i równoczesnego zobowiązania się do zachowania w tajemnicy informacji związanych z ich przetwarzaniem – wzór załącznik **nr 2** do niniejszej instrukcji,
3) wydanie przez Administratora stosownego upoważnienia do przetwarzania danych osobowych - wzór załącznik **nr 3** do niniejszej instrukcji.
4) wydanie przez Administratora stosownego upoważnienia do przetwarzania danych osobowych i rozpatrywania wniosków o udostępnienia danych w celu innych niż włączenie do zbioru – wzór załącznik **nr 4** do niniejszej instrukcji.

2. Z chwilą zarejestrowania użytkownika w systemie, użytkownik jest informowany przez ABI o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.
3. Dokumenty, o których mowa w § 11 ust.1 podlegają przechowaniu w ewidencji prowadzonej przez ABI.

§ 12

1. Z chwilą utraty przez Użytkownika prawa dostępu do systemów i przetwarzanych danych ABI na polecenie Administratora, w zależności od zaistniałej sytuacji ma obowiązek niezwłocznie:

    1) w przypadku ustania zatrudnienia użytkownika u Administratora – wyrejestrować użytkownika z systemu, wykreślić jego Identyfikator z ewidencji i unieważnić hasło.
    2) w przypadku zmiany zakresu obowiązków użytkownika – stosownie skonfigurować dostępy do systemów, baz danych i przetwarzanych informacji.

2. Wszelkie zmiany danych podlegają odnotowaniu w stosownej ewidencji.

Rozdział 5
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

§ 13

1. Osobą odpowiedzialną za sposób ustalania, przechowywania i wprowadzania haseł dostępu dla użytkowników jest ABI.

2. Pierwsze hasło dostępu, nadawane jest przez ABI wraz z identyfikatorem użytkownikowi uprawnionemu. Każde kolejne hasło dostępu użytkownik zmienia sam zgodnie z wymogami systemu i ma obowiązek jego zapamiętania oraz nie przekazywania osobom trzecim lub innym użytkownikom.

3. W wypadku stwierdzenia podejrzenia lub ujawnienia hasła użytkownika osobom trzecim, użytkownik ma obowiązek natychmiastowej zmiany hasła z poinformowaniem o tym fakcie ABI.

4. Hasła dostępu zapisywane są na ekranie monitora w formie niejawnej.

5. System narzuca minimalną ilość znaków w haśle oraz obowiązek jego zmiany co 30 dni.

§ 14

1. Dane osobowe gromadzone są wyłącznie na wyznaczonych nośnikach danych. Zabrania się gromadzenia danych osobowych na innych nośnikach danych.

2. Tworzy się rejestr nośników aktywnych jak i bezpieczeństwa na których przetwarzane są dane osobowe.

3. Rejestr o którym mowa w ust. 2 prowadzi Administrator Bezpieczeństwa Informacji.

Rozdział 6.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

§ 15

1. Użytkownik rozpoczynający pracę zobowiązany jest do przestrzegania procedur, które mają na celu sprawdzenie stanowiska pracy co do wskazania bytności osób nieuprawnionych, a w szczególności:

    1) sprawdzenie przed wejściem do pomieszczenia czy na drzwiach, zamkach nie ma widocznych śladów prób niepowołanego ich otwierania,
    2) sprawdzenie stanu okien, ich zamknięcia,
    3) sprawdzenie stanu sprzętu informatycznego oraz zamknięcia szaf i biurek,
    4) po włączeniu komputera ocena jakości jego pracy i ewentualnych zmian.

2. Użytkownik przed przystąpieniem do przetwarzania danych musi zalogować się w systemie, posługując się swoim identyfikatorem i hasłem.

3. Po zalogowaniu się w systemie użytkownik ma obowiązek ocenić pracę systemu i stan zbioru danych a w przypadku jakichkolwiek wątpliwości zgłosić ten fakt ABI lub ASI.

4. W trakcie pracy z systemem Użytkownik powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie a w szczególności:

    1) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób nieuprawnionych,
    2) dopilnować aby w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych nie przebywały jakiekolwiek osoby trzecie, a jeśli przebywają to tylko za zgodą przełożonych i w obecności osób uprawnionych,
    3) stosować wygaszacze ekranów, które włączają się po upływie 10 minut bezczynności komputera, wygaszacz powinien być blokowany hasłem.

§ 16

1. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu.

2. Zabrania się opuszczenia stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem ust.1.

3. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:

    1) wylogować się z systemu i zaczekać na jego wyłączenie się,
    2) sprawdzić czy nie zostały pozostawione bez nadzoru jakiekolwiek nośniki informacji, tj. dyskietki, taśmy, płyty, wydruki, teczki, itp.
    3) upewnić się, że szafy i biurka z dokumentacją są zamknięte,
    4) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie a klucze złożyć w miejscu do tego przeznaczonym.

4. Po godzinach pracy Administrator powinien zapewnić ochronę pomieszczeń jednostki w których przetwarzane są dane osobowe w formie fizycznej, elektronicznej lub jakiejkolwiek innej zgodnej z przepisami prawa.

Rozdział 7.
Tworzenie i przechowywanie kopii awaryjnych, nośników informacji, wydruków.

§ 17

Kopiowanie danych osobowych na nośniki informacji, robienie wydruków oraz wykorzystywanie tych danych w celach innych niż wynikające z nałożonych na użytkowników obowiązków lub wynikających z odrębnych przepisów prawa jest zabronione.

§ 18

1. Kopie awaryjne należy wykonywać codziennie. Kopię wykonuje ASI. Po wykonaniu kopii ASI ma obowiązek sprawdzenia jej poprawności i przydatności w przypadku z niej skorzystania.

2. ASI ma obowiązek opracować stosowny dokument określający procedurę wykonywania kopii awaryjnych. Kopie awaryjne wykonuje ASI zgodnie z opracowaną i zatwierdzoną przez Administratora procedurą. Po wykonaniu kopii ASI ma obowiązek sprawdzenia poprawności jej wykonania i przydatności w przypadku potrzeby z niej skorzystania.

3. Kopie awaryjne przechowuje ABI, w miejscach wskazanych przez Administratora, zapewniając im odpowiednie warunki bezpieczeństwa. Muszą to być pomieszczenia inne niż te w których przechowuje się lub przetwarza zbiory danych osobowych.

4. Kopie awaryjne danych, jeśli nie stanowią inaczej przepisy prawa należy przechowywać przez miesiąc od utworzenia.

5. Zdezaktualizowane i uszkodzone kopie awaryjne ASI ma obowiązek mechanicznie zniszczyć w sposób uniemożliwiający ich ponowne użycie.

§ 19

1. Nośniki informacji, w tym kopie danych i wydruki komputerowe przechowuje się wyłącznie wówczas, gdy jest to konieczne i dozwolone przepisami prawa. Przechowuje się je w wyznaczonych pomieszczeniach w szafach i innych meblach biurowych, które posiadają odpowiednie zamknięcia, uniemożliwiające niepowołany dostęp do nich osób trzecich.

2. Pomieszczenia, o których mowa w ust.1 winny spełniać określone warunki bezpieczeństwa, a w szczególności posiadać:

    1) wewnętrzne ściany, gwarantujące trwałe oddzielenie ich od innych pomieszczeń,
    2) pełne drzwi wejściowe, zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania (patentowy lub szyfrowy),
    3) odpowiednie zabezpieczenie okien przed dostępem z zewnątrz i obserwacją.

3. W razie uzasadnionej potrzeby ABI wprowadza dalej idące środki bezpieczeństwa dotyczące przechowywania nośników informacji w szafach i innych meblach biurowych, które winny być:

    1) zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania, tj. w szczególności zamek patentowy lub szyfrowy,
    2) po zakończeniu pracy zamknięte klucze złożone w przeznaczonym do tego miejscu.

§ 20

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe,
   przeznaczone do:

   1) likwidacji – pozbawia się wcześniej zapisanych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie,
   3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora danych.

2. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

Rozdział 8.
Ochrona systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

§ 21

1. W celu ochrony systemów i danych w nich przetwarzanych na każdym komputerze należy zainstalować działający w „tle” program antywirusowy. Program antywirusowy musi zostać skonfigurowany w taki sposób, aby jak najefektywniej zabezpieczyć dane , w szczególności automatycznie sygnalizować obecność wirusów, nie dopuszczać możliwości zapisywania podejrzanych plików danych, 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 tych wykorzystywanych do celów instalacyjnych.

3. Obowiązkiem ASI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego zgodnie z jego wymogami konfiguracyjnymi oraz przeprowadzanie okresowych kontroli komputerów co do poprawności działania programów antywirusowych.

4. W przypadku stwierdzenia ingerencji oprogramowania obcego – wirusów, ASI musi dołożyć wszelkich starań w celu usunięcia tych plików, usunięcia ewentualnych skutków ich działania i prawidłowego zabezpieczenia sprzętu i danych.

5. Przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej system jest chroniony zasilaczami awaryjnymi.

Rozdział 9.
Informacje o odbiorcach, którym dane osobowe zostały udostępnione.

§ 22

1. Tworzy się centralną ewidencję udostępnień danych odbiorcom, w rozumieniu **art.7, pkt 6** ustawy o ochronie danych osobowych, prowadzoną w formie elektronicznej oraz papierowej przez ABI.

2. Każde udostępnienie musi zostać odnotowane w centralnej ewidencji o której mowa w ust.1 z uwzględnieniem informacji o:

    1) danych odbiorcy,
    2) dacie udostępnienia,
    3) zakresie i przeznaczeniu udostępnienia.

3. Osoby upoważnione do udostępniania danych są zobowiązane do zgłoszenia faktu udostępniania danych Administratorowi Bezpieczeństwa Informacji, który ma obowiązek dokonać stosownych wpisów w centralnej ewidencji udostępnień.

Rozdział 10.

Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 23

1. Okresowe przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu niezbędne dla prawidłowego funkcjonowania jednostki wykonuje ASI lub inna osoba upoważniona przez Administratora danych.

2. 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.

3. 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.

§ 24

1. Tworzy się ewidencję osób upoważnionych do wykonywania prac o których mowa w § 23 niniejszej instrukcji.

2. Tworzy się ewidencję przeglądów i konserwacji, która w winna posiadać pola tj.;: nazwa systemu, opis procedury, zakres przeglądu, nazwisko osoby uprawnionej do wykonania przeglądu, data wykonania przeglądu.

3. Ewidencje o której mowa w § 24 ust.1 i 2 prowadzi w formie papierowej i elektronicznej Administrator Bezpieczeństwa Informacji.

Rozdział 11.
Postępowanie w zakresie komunikacji w sieci komputerowej.

§ 25

1. Komunikacja w sieci komputerowej jest dozwolona tylko po odpowiednim zalogowaniu się i podaniu indywidualnego hasła użytkownika.

2. ASI poprzez odpowiednią konfiguracje elementów sieci uniemożliwia osobom nieupoważnionym podłączanie urządzeń komputerowych innych niż będące na wyposażeniu Urzędu Gminy Miłkowice. Podłączenie nowego urządzenia jest możliwe w porozumieniu z ASI.

3. Wprowadzenie 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.

4. Konfiguracja sieci jest wykonywana przez ASI na wniosek ABI. Wszelkie zmiany konfiguracji systemu podlegają ewidencji, którą prowadzi ABI.

Rozdział 12.
Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych.

§ 26

1. Naruszenie ochrony danych osobowych, może być spowodowane:

1) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.,

2) 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,

3) 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:

1) 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.,

2) brak dostępu do zawartości zbioru danych – zbiór istnieje lecz nie można go otworzyć,

3) zmienioną zawartość zbioru, niepoprawną treść, postać, datę, różnicę w danych itp.,

4) 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,

5) różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji,

6) zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych,

7) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych,

8) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione,

9) próba nielegalnego logowania się do systemu lub włamania do systemu,

10) zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych.

3. Niniejszą Instrukcję 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.

§ 27

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w § 26 niniejszej Instrukcji, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz ABI lub osobę upoważnioną przez ABI.

§ 28

Użytkownik do momentu przybycia ABI lub osoby przez niego upoważnionej powinien:

1) zabezpieczyć dostęp do pomieszczenia lub urządzenia,

2) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony,
3) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony,
4) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych,

§ 29

1. ABI po otrzymaniu informacji o naruszeniu lub próby naruszenia zabezpieczeń systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia.

2. Po przybyciu na miejsce, o którym mowa w ust.1 ABI realizuje czynności w kolejności:

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

§ 30

1. ABI z przebiegu zdarzenia sporządza notatkę służbową, która obejmuje:

1) dane osoby stwierdzającej naruszenie ochrony,
2) datę, godzinę i miejsce naruszenia ochrony,
3) rodzaj naruszenia ochrony,
4) czas powiadomienia o zdarzeniu,
5) opis podjętych czynności,
6) wnioski do realizacji,

2. Notatkę o której mowa w ust.1 ABI przekazuje Administratorowi lub osobie upoważnionej przez niego.

§ 31

Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych, udziela ABI lub ASI.

§ 32

Dokonywanie zmian w miejscu naruszenia ochrony bez zgody, o której mowa w § 31 jest dopuszczalne tylko w wypadku konieczność ratowania osób, mienia albo zapobieżenia powstaniu innego niebezpieczeństwa.

§ 33

1. W przypadku powołania doraźnego zespołu, o którym mowa w § 29 ust. 2 pkt.5 , pracą jego kieruje ABI.
2. 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.
3. Protokół zawierać powinien wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości naruszeniom ochrony danych osobowych.

4. Protokół przekazywany jest Administratorowi lub osobie upoważnionej przez niego w celu akceptacji wniosków i zaleceń usprawniających zabezpieczenia ochrony danych.

§ 34

W przypadku stwierdzenia:

1) błędu użytkownika systemu – ABI przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej;

2) uaktywnienia wirusa – ABI ustala źródło jego pochodzenia oraz uaktualni zabezpieczenia antywirusowe;

3) zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa;

4) włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę;

5) złego stanu urządzenia lub złego działania programu – należy przeprowadzić kontrolę czynności serwisowo-programowych.

Rozdział 13.
Postanowienia końcowe.

§ 35

1. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI w porozumieniu z ABI.

2. ABI prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych" w Urzędzie Gminy Miłkowice.

3. ABI dokonuje sprawdzenia sprawności funkcjonowania zabezpieczeń systemów, w których przetwarzane są dane osobowe, nie rzadziej niż raz na 6 miesięcy. Z przeprowadzonych kontroli sporządza notatkę służbową, którą przedkłada Administratorowi.

§ 36

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

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

§ 37

W sprawach nie uregulowanych 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 rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29

kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz.1024).