Zarządzenie Nr 1/2005
Starosty Wąbrzeskiego
z dnia 28 stycznia 2005 roku

w sprawie wyznaczenia administratora bezpieczeństwa informacji, wprowadzenia do użytku służbowego instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz polityki bezpieczeństwa

Na podstawie art 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U z 2002 r. Nr 101 poz. 926 z późn. zm.) oraz 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku (Dz. U. 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

Zarządzam co następuje:

§1

Wyznaczam Pana Tomasza Ścigniejew jako Administratora Bezpieczeństwa Informacji

§ 2

Wprowadzam do użytku służbowego :

- „Instrukcje zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w brzmieniu stanowiącym załącznik nr 1 do zarządzenia

§ 3

Wprowadzam do użytku służbowego :

- „Politykę bezpieczeństwa" w brzmieniu stanowiącym załącznik nr 2 do zarządzenia

§ 4

Dokumentację, o której mowa § 2 i 3 wdraża Administrator Danych.

§ 5

Zobowiązuję pracowników przetwarzających dane osobowe do przestrzegania zasad określonych w dokumentacji o której mowa § 2 i 3 .

§ 6

Zobowiązuję Kierowników Wydziałów Starostwa Powiatowego w Wąbrzeźnie, w których przetwarzane są dane osobowe do sprawowania nadzoru nad ich ochroną oraz do współpracy w tym zakresie z Administratorem Bezpieczeństwa Informacji.

§ 7

Traci moc Zarządzenie Nr 8/99 Starosty Wąbrzeskiego z dnia 17 września 1999 roku w sprawie wyznaczenia administratora bezpieczeństwa informacji, instrukcji postępowania w przypadku naruszenia tajemnicy ochrony danych w Starostwie Powiatowym w Wąbrzeźnie oraz w sprawie instrukcji zarządzania systemem informatycznym ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji Starostwa Powiatowego w Wąbrzeźnie oraz Zarządzenie Nr 9/2001 Starosty Wąbrzeskiego z dnia 05 października 2001 roku w sprawie zmiany Zarządzenia Nr 8/99 z dnia 17 września 1999 roku

§ 8

Zarządzenie wchodzi w życie z dniem podpisania.

Starosta
mgr Krzysztof Mackiewicz

załącznik Nr 1 do zarządzenia Nr 1/2005
Starosty Wąbrzeskiego z dnia
28 stycznia 2005 roku

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

§ 1

Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wąbrzeźnie.

§ 2

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności.

1. Starosta Powiatowy jako administrator danych osobowych (ADO) wyznacza administratora bezpieczeństwa informacji (ABI).

2. ABI jest odpowiedzialny za bezpieczeństwo danych osobowych w systemie informatycznym Starostwa. Prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych- administratora systemu informatycznego, użytkowników uprzywilejowanych, użytkowników.

3. ADO na wniosek ABI upoważnia osobę (ASI) do administrowania systemem informatycznym, której zadaniem jest utrzymanie i konserwacja systemów informatycznych, tworzenie kont użytkowników, przydzielanie i modyfikacja ich uprawnień, nadawanie identyfikatorów i haseł dostępu do systemu informatycznego na poziomie systemu operacyjnego. Dokonuje czynności prowadzące do zmiany haseł przez użytkowników (U) w systemach wyposażonych w system wymuszających zmianę haseł przez U. ASI jest zobowiązany do przekazania ADO w formie pisemnej kompletu identyfikatorów i haseł dostępu do systemu informatycznego – operacyjnego i użytkowego- zarówno ASI, UU, U, nośników instalacyjnych systemu operacyjnego i systemów informatycznych instalowanych w Starostwie.
   Wycofania upoważnienia może nastąpić na wniosek ABI lub z urzędu.

4. ADO na wniosek ASI upoważnia osoby jako użytkowników uprzywilejowanych (UU) na poziomie administratorów systemów informatycznych, nadaje lub modyfikuje uprawnienia UU do zasobów systemu informatycznego, określa identyfikator i hasło. Techniczny aspekt wyżej wymienionych spraw realizuje ASI.
   UU określają identyfikatory , hasła i uprawnienia na poziomie administratorów systemów informatycznych dla użytkowników (U).
   Wycofania upoważnienia następuje na wniosek ABI lub ASI.

5. ADO na wniosek kierownika jednostki organizacyjnej wykorzystującej systemy informatyczne upoważnia osobę (U) do przetwarzania danych osobowych, nadaje lub modyfikuje uprawnienia użytkownika do zasobów systemu informatycznego. Identyfikatory , hasła i uprawnienia na poziomie administratorów systemów

informatycznych dla użytkowników (U) określa ASI lub UU. Techniczny aspekt wyżej wymienionych spraw realizuje ASI.
Wycofania upoważnienia następuje na wniosek ABI , kierownika jednostki , ASI lub z urzędu.

6. W wypadkach awaryjnych ABI w razie konieczności udostępnia ASI, UU lub podmiotom realizującym usuwanie awarii zdeponowane identyfikatory i hasła dostępu do systemu informatycznego zarówno administratora, użytkowników uprzywilejowanych (UU) i użytkowników (U), nośników instalacyjnych systemu operacyjnego i systemów informatycznych instalowanych w Starostwie.

§ 3

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

1. Hasła wszystkich użytkowników systemu informatycznego deponowane w formie pisemnej u ABI.

2. Hasło używane do uwierzytelniania użytkowników ma być zmieniane nie rzadziej niż co 30 dni i musi składać się co najmniej z 8 znaków.

3. ASI jest zobowiązany do przydziału identyfikatorów i haseł do systemu informatycznego na poziomie dostępu do systemu operacyjnego oraz zmian w systemie informatycznym użytkowym posiadającym moduł wymuszania zmian haseł dla użytkowników i poinformowania o zmianach ABI, UU, U.

4. UU jest zobowiązany do przydział identyfikatorów i haseł do systemu informatycznego na poziomie oprogramowania użytkowego i poinformowania o zmianach ABI, U.

5. U jest zobowiązany do zabezpieczenia używanego przez siebie hasła przed użyciem przez osoby nieupoważnione.

6. Zaleca się wykorzystywanie możliwości systemów operacyjnych do zabezpieczeń stacji roboczych wyposażonych w systemy operacyjne o właściwościach podobnych do Windows 2000/XP oraz Liunux pod warunkiem zdeponowania indentyfikatora i hasła u ABI.

7. Stosowanie nie uzgodnionych z ABI sposobów i form zabezpieczeń systemu informatycznego jest zabronione.

§ 4

Procedury rozpoczęcia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Czynności jakie należy wykonać w celu uruchomienia systemu informatycznego:
- włączenie źródła zasilania
- uruchomienie stacji roboczej - zalogowanie się do sieci LAN

- uruchomienie systemu informatycznego z wykorzystaniem mechanizmów uwierzytelniania wykorzystywanych przez oprogramowanie użytkowe.

W celu zakończenia pracy z systemem informatycznym należy wykonać powyższe czynności w odwrotnej kolejności.

2. W sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieupoważniona osoba należy niezwłocznie przerwać wykonywane operacje i czynności, następnie zakończyć pracę z systemem informatycznym służącym do przetwarzania danych.

3. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego oraz gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać naruszenie zabezpieczeń tych danych należy niezwłocznie podjąć próbę ustalenia ilości utraconych lub przejętych bezprawnie informacji z bazy i poinformować bezpośredniego przełożonego oraz ABI o stwierdzonym fakcie.

4. ABI uzyskaną informację od pracowników lub Kierowników poddaje analizie w celu ustalenia okoliczności utraty danych zgodnie z obowiązującym stanem prawnym.

5. W przypadku ustalenia, że została naruszona tajemnica ochrony danych osobowych ABI przygotowuje wniosek do organów ścigania oraz Generalnego Inspektora Ochrony Danych o podjęcie stosownych działań w związku ze stwierdzonym faktem naruszenia postanowień ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (jednolity tekst Dz.U z 2002 roku Nr 101, poz.926, ze zmianami) i przedkłada do akceptacji Staroście .
   Wniosek po zatwierdzeniu przez Starostę , ABI przekazuje niezwłocznie wyżej wymienionym organom.

6. W przypadku włamania do Starostwa i stwierdzenia naruszenia tajemnicy ochrony danych względnie powzięcia podejrzeń osoba – pracownik , który stwierdził ten fakt informuje o nim Starostę lub jego Zastępcę oraz ABI , którzy podejmują niezbędne działania zgodnie z niniejszą instrukcją.

§ 5

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Kopie zapasowe danych oraz systemu informatycznego używanego do ich przetwarzania wykonuje ABI.

2. Kopie zapasowe danych wykonuje się nie rzadziej niż raz w tygodniu, a wypadku zintensyfikowania procesu zasilania baz danych na wniosek kierowników jednostek, UU lub ASI powinny być wykonywane z częstotliwością odpowiednią do przyrostu danych w bazie.

3. Kopie zapasowe systemu informatycznego używanego do przetwarzania danych wykonuje się nie rzadziej niż raz w miesiącu oraz bezpośrednio przed i po każdej modernizacji i aktualizacji systemu.

4. Kopie zapasowe danych oraz systemu informatycznego używanego do ich przetwarzania zabezpiecza się za pomocą utrwalenia na nośnikach magnetycznych CD.

§ 6

Sposób, miejsce i okres przechowywania kopii zapasowych oraz elektronicznych nośników informacji zawierających dane osobowe.

1. Kopię zapasowe danych oraz systemu informatycznego używanego do ich przetwarzania utrwalone na nośnikach magnetycznych CD należy przechowywać w wydzielonej kasecie w ogniotrwałej szafie pancernej < trezor > znajdującej się w pokoju Nr 1.

2. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający ich odczytanie.

3. Elektroniczne nośniki informacji wycofane z eksploatacji, a nie przeznaczone do zniszczenia należy pozbawić zawartości w sposób uniemożliwiający odczytanie zapisanych na nich danych.

§ 7

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. Stacje robocze wykorzystywane do obsługi systemów informatycznych w których przetwarza się dane osobowe narażone są na działalność oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego – wirusy, trojany, keylogery, spyware i inne (WTKS). Szczególnie narażone są komputery wyposażone w stacje dyskietek, czytniki CD lub dostęp do internetu. Należy wyeliminować możliwość jednoczesnego korzystania z powyższych rozwiązań technicznych z dostępem do systemów informatycznych służących do przetwarzania danych.

2. W celu wyeliminowania potencjalnego zagrożenia ASI wdroży system zabezpieczeń antywirusowych co najmniej jednego z dostawców tego typu oprogramowania z możliwością automatycznej aktualizacji bazy wirusów.

3. Wszyscy użytkownicy systemu informatycznego zobowiązani są do skanowania systemu pod kątem obecności WTKS przed każdorazowym zalogowaniem się do systemów informatycznych służących do przetwarzania danych.

4. Niedozwolone jest indywidualne instalowanie na stanowiskach roboczych oprogramowania niezwiązanego z obsługą systemów informatycznych służących do przetwarzania danych.

§ 8

Sposób realizacji wymogów, o których mowa w § 7 ust.1 pkt. 4 tj. informacji o odbiorcach, którym dane te zostały udostępnione, dacie i zakresie tego udostępnienia.

1. Przy przetwarzaniu danych osobowych należy wykorzystywać wbudowane w systemy informatyczne mechanizmy zapewniające odnotowanie informacji o udostępnieniach danych odbiorcom, w rozumieniu art. 7 pkt. 6 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (jednolity tekst Dz.U z 2002 roku Nr 101, poz.926, ze zmianami).

§ 9

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

1. Celem wykonywania przeglądów i konserwacji systemów służących do przetwarzania danych jest ich bezawaryjna praca umożliwiająca zachowanie integralności i spójności danych, zapewnienie ich przetwarzania i odzyskiwania w sytuacjach awaryjnych.

2. Przeglądy systemu dokonywane są okresowo przynajmniej raz w tygodniu pod kątem obecności WTKS.

3. ASI dokonuje nie rzadziej niż raz w miesiącu wyrywkowy przegląd stacji roboczych wykorzystywanych do przetwarzania danych pod kątem zainstalowanych programów nie służących przetwarzaniu danych. Informacje w formie pisemnej przedstawia ABI .

4. W wypadku stwierdzenia awarii systemu, utraty danych , zauważonych przekłamań w bazach danych ASI wraz z ABI dokonują analizy zaistniałej sytuacji awaryjnej, określają przyczynę, przeprowadzają niezbędne czynności w celu wyeliminowania stwierdzonych nieprawidłowości, dokonują niezbędne zmiany w procedurach. Naprawiają system informatyczny na podstawie wykonanej kopii zapasowej zbiorów i systemów.

5. Osoba uprawniona do przeglądów i konserwacji systemu informatycznego jest ABI oraz ASI.

6. W przypadku wypadku gdy zaistnieje konieczność zlecenia tych czynności osobom nie posiadającym upoważnień do przetwarzania danych wszelkie czynności muszą być wykonywane w obecności ABI lub ASI.

7. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy należy pozbawić wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawić je pod nadzorem osoby upoważnionej przez ADO.

załącznik Nr 2 do zarządzenia Nr 1/2005
Starosty Wąbrzeskiego z dnia
28 stycznia 2005 roku

Polityka bezpieczeństwa.

§ 1

Wprowadzenie

1. Politykę bezpieczeństwa należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych w Starostwie Powiatowym w Wąbrzeźnie.

2. Polityka bezpieczeństwa odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych.

3. Celem polityki bezpieczeństwa, jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych przy wsparciu osób zatrudnionych w Starostwie.

§ 2

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1. Obszar w którym przetwarza się dane osobowe stanowi cały budynek położony w Wąbrzeźnie przy ulicy Wolności 44 zajmowany przez Starostwo Powiatowe w Wąbrzeźnie (z wyłączeniem ciągów komunikacyjnych, pomieszczeń gospodarczych oraz pomieszczeń wynajmowanych innym podmiotom).

2. Przetwarzaniem danych osobowych nazywamy 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.

3. Zmiany pomieszczeń wykorzystywanych przez Wydziały Starostwa oraz techniczne możliwości rozwoju sieci, w tym również bezprzewodowej powodują, że praktycznie każde z pomieszczeń Starostwa Powiatowego w Wąbrzeźnie jest wykorzystywane lub może być wykorzystywane do przetwarzania danych osobowych.

§ 3

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

1. Do przetwarzania danych osobowych w Starostwie Powiatowym w Wąbrzeźnie stosuje się następujące systemy informatyczne:
   - Program EGB V win do prowadzenia ewidencji gruntów i budynków
   - pakiet RADIX w którego skład wchodzą systemy :WIP system windykacji opłat i podatków, FKB system planowania budżetu, FPB system finansowo-księgowy księgowości budżetowej, KASA system obsługi kasy, KADRY I PŁACE oraz UPR.
   - Program ewidencji pojazdów A-Soft ver. 10.18.

2. W Starostwie Powiatowym w Wąbrzeźnie przetwarzane są następujące zbiory danych osobowych - w sposób tradycyjny (T) oraz za pomocą systemów informatycznych (I) :
   - ewidencja gruntów (I- EGBVwin),
   - ewidencja wieczystych użytkowników gruntów Skarbu Państwa i Powiatu (T),
   - wykaz budynków mieszkalnych i niemieszkalnych oraz obiektów zbiorowego zakwaterowania przekazanych do użytku (T),
   - ewidencja wydanych pozwoleń na budowę (T),
   - rejestr zalesień (T),
   - księga wodna (T),
   - rejestr łodzi rybackich (T),
   - rejestr kart wędkarskich (T),
   - ewidencja opłat melioracyjnych (T),
   - rejestr o dopuszczalnej emisji (T),
   - ewidencja osób mających zobowiązania wobec Skarbu Państwa i Powiatu (I - Radix),
   - ewidencji pojazdów (I – A-Soft ver. 10.18),
   - ewidencja kierowców (dawniej -rejestr wniosków ,zawiadomień i zamówień na prawa jazdy i świadectwa klasyfikacji) (T),
   - rejestr tablic rejestracyjnych (T),
   - rejestr dowodów rejestracyjnych(T),
   - rejestr wydanych międzynarodowych praw jazdy(T),
   - rejestr osób które zmieniły imię lub nazwisko(T),
   - listy poborowych(T),

§ 4

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. W zbiorze danych „ ewidencja gruntów" przetwarzane są dane osobowe podmiotów w zakresie:
   - danych adresowych : nazwiska i imiona,imiona rodziców, adres zamieszkania lub pobytu,numer ewidencyjny PESEL, numer identyfikacji podatkowej NIP,

- posiadanych przez podmioty nieruchomości.

2. W zbiorze danych „ewidencja osób mających zobowiązania wobec Skarbu Państwa i Powiatu" przetwarzane są dane osobowe podmiotów w zakresie :
   - danych adresowych : nazwiska i imienia, adresu zamieszkania lub pobytu,
   - zobowiązań do świadczeń pieniężnych wobec Skarbu Państwa lub Powiatu

3. W zbiorze danych „ewidencji pojazdów" przetwarzane są dane osobowe podmiotów w zakresie:
   - danych adresowych : nazwiska i imiona, adres zamieszkania lub pobytu
   - posiadanych przez podmioty pojazdach

§ 5

Sposób przepływy danych pomiędzy systemami.

1. Przetwarzanie danych w programie EGBVwin przeznaczonym do prowadzenia ewidencji gruntów odbywa się w bazach danych tworzonych na serwerze Perwasive V8. Są to wielotablicowe relacyjne bazy danych. Algorytm przepływu danych między tablicami nie jest upubliczniony i nie stanowi przedmiotu opisu w instrukcji obsługi ani specyfikacji technicznej oprogramowania EGBVwin. Dane z systemu nie zasilają w sposób dynamiczny zewnętrznych baz danych.

2. Przetwarzanie danych w programie Radix przeznaczonym do prowadzenia ewidencji osób mających zobowiązania wobec Skarbu Państwa i Powiatu odbywa w środowisku baz danych dBase. Są to wielotablicowe relacyjne bazy danych. Algorytm przepływu danych między tablicami nie jest upubliczniony i nie stanowi przedmiotu opisu w instrukcji obsługi ani specyfikacji technicznej oprogramowania . Dane z systemu nie zasilają w sposób dynamiczny zewnętrznych baz danych.

3. Przetwarzanie danych w programie A-Soft ver. 10.18 przeznaczonym do prowadzenia ewidencji pojazdów odbywa w środowisku baz danych Btrieve. Są to wielotablicowe relacyjne bazy danych. Algorytm przepływu danych między tablicami nie jest upubliczniony i nie stanowi przedmiotu opisu w instrukcji obsługi ani specyfikacji technicznej oprogramowania S-Soft. Dane z systemu nie zasilają w sposób dynamiczny zewnętrznych baz danych.

4. Urządzenia służące do przetwarzania danych w systemach informatycznych Radix i EGBVwin są jednocześnie wykorzystywane do połączenia z siecią internet. System A-Soft działa na jednym stanowisku i nie jest połączony z siecią LAN (Local Area Network) , WAN (Wide Area Network) oraz MAN (Metropolitan Area Network).

5. Uwzględniając wielofunkcyjną specyfikę wykorzystywania urządzeń informatycznych w Starostwie Powiatowym w Wąbrzeźnie na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom zabezpieczeń.

§ 6

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Obszar, o którym mowa w § 2 Polityki bezpieczeństwa, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 2 Polityki bezpieczeństwa , jest dopuszczalne za zgodą administratora danych (ADO) lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3. W systemach informatycznych służących do przetwarzania danych osobowych należy wykorzystywać wbudowane mechanizmy kontroli dostępu do danych.

4. Należy zapewnić rejestracje w systemie informatycznym odrębnego identyfikatora dla każdego uprawnionego użytkownika.

5. Dostęp do danych może być możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

6. Systemy informatyczny służący do przetwarzania danych osobowych oraz systemy operacyjne należy zabezpieczyć przed:
   - działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
   - utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

7. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

8. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło powinno składać się co najmniej z 8 znaków.

9. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

10. Kopie zapasowe:
    - przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
    - usuwa się niezwłocznie po ustaniu ich użyteczności.

11. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza

siedzibą Starostwa Powiatowego, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

12. Urządzenia, dyski lub inne elektroniczne nośniki informacji, 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;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

13. Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

14. Hasła stosowane do uwierzytelniania w systemach informatycznych muszą składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

15. Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

16. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w punkcie 15, obejmują one:
    - kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
    - kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.