STAROSTA
WARSZAWSKI ZACHODNI
z siedzibą
w Ożarowie Mazowieckim

ZARZĄDZENIE NR 95 / 2012
STAROSTY WARSZAWSKIEGO ZACHODNIEGO
z dnia 18 grudnia 2012 r.

w sprawie wprowadzenia „Instrukcji zarządzania systemem informatycznym Starostwa Powiatu Warszawskiego Zachodniego"

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U z 2001 r. Nr 142, poz. 1592 z późn. zm.) oraz § 3 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. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. Wprowadzam do stosowania „Instrukcję zarządzania systemem informatycznym Starostwa Powiatu Warszawskiego Zachodniego" stanowiącą załącznik do niniejszego Zarządzenia.

§ 2. Tracą moc Zarządzenia: Nr 20/2006 z dnia 12 czerwca 2006 r. oraz Nr 54/2008 z dnia 31 grudnia 2008 r.

§ 3. Nadzór na wykonaniem niniejszego Zarządzenia powierzam Administratorowi Sieci Informatycznej.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od dnia 1 stycznia 2013 r.

STAROSTA
Jan Zychliński

INSTRUKCJA ZARZADZANIA SYSTEMEM INFORMATYCZNYM STAROSTWA POWIATU WARSZAWSKIEGO ZACHODZNIEGO

Wydanie 2		**Pieczęć firmowa:**	
		STAROSTWO POWIATU WARSZAWSKIEGO ZACHODNIEGO 05-850 Ożarów Mazowiecki ul. Poznańska 129/133 tel.: 22 733-72-00, fax: 22 733-72-01	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
INFORMATYK Zbigniew Rębis	**14.12.2012 r.**	STAROSTA Jan Zychliński	**18.12.2012 r.**

ROZDZIAŁ I

Wstęp

§1

1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych zwana dalej „Instrukcją", określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji a także zasady i tryb postępowania Administratora Danych oraz osób przez niego upoważnionych przy przetwarzaniu danych osobowych.
2. Instrukcja została opracowana zgodnie z wymogami określonymi w §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§2

Instrukcja określa stosowne procedury i warunki zarządzania systemem informatycznym oraz kartotekami zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożenia oraz kategorii danych objętych ochroną.

ROZDZIAŁ II

Definicje

1. Ilekroć w Instrukcji jest mowa o:
   1) **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,

2) **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,

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

4) **kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej zawierającej dane osobowe,

5) **Administratorze Danych** - rozumie się przez to Starostę Warszawskiego Zachodniego,

6) **Administratorze Bezpieczeństwa Informacji** - rozumie się przez to osobę odpowiedzialną za stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności za zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń, upoważnioną do nadzoru i kontroli w zakresie określonym przepisami o ochronie dartych osobowych oraz regulacjami wewnętrznymi Administratora Danych,

7) **Administrator Sieci Informatycznej** - osoba odpowiedzialna za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację,

8) **komórce organizacyjnej** - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną zgodnie z regulaminem organizacyjnym,

9) **użytkowniku** — rozumie się przez to osobę upoważnioną przez Starostę, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadającą ustalony identyfikator i hasło,

10) **pomieszczeniach** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

ROZDZIAŁ III

Zabezpieczanie systemu

§3

Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemu informatycznego.

§4

1. W celu uwzględnienia ewentualnych zagrożeń oraz kategorii przetwarzanych danych wprowadza się, następujące poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:

   1) podstawowy,

   2) podwyższony,

   3) wysoki.

2. Poziom, co najmniej podstawowy stosuje się, gdy w systemie informatycznym nie są przetwarzane dane, o których mowa w art.27 ustawy o ochronie danych osobowych, oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

3. Poziom, co najmniej podwyższony stosuje się, gdy w systemie informatycznym są przetwarzane dane, o których mowa w art.27 ustawy o ochronie danych osobowych oraz żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych jest połączone z siecią publiczną.

§5

1. Realizację zamierzeń powinny zagwarantować następujące założenia:

   1) wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za ochronę tych danych,

   2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,

   3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do poziomów baz danych osobowych — stosownie do indywidualnego zakresu upoważnienia,

   4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń okresowe poprzez sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,

   5) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,

   6) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych, wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

2. Przez politykę bezpieczeństwa należy rozumieć określenie zadań, które należy zastosować dla zapewnienia spójności wszystkich zabezpieczeń danych osobowych. Została ona sformułowana w „Polityce Bezpieczeństwa" wprowadzonej odrębnym zarządzeniem Starosty oraz w kolejnych rozdziałach niniejszej instrukcji. Odzwierciedla ona podstawowe zasady bezpieczeństwa, a także zarządzania systemem informatycznym oraz kartotekami u Administratora Danych.

ROZDZIAŁ IV

Przydział uprawnień i identyfikatorów

§6

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie. Wzór upoważnienia do dostępu do danych osobowych i do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych stanowi **załącznik nr 1 do instrukcji.**

2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.

3. Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.

4. Postanowienia ust. 2 nie dotyczą użytkowników, którzy jako jedyni mają dostęp do danych przetwarzanych w systemie informatycznym oraz do użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.

5. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia ewidencji przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do zbiorów danych oraz dokonywaniem zmian w zakresie przyznanych uprawnień.

6. Pracownicy Zespołu ds. kadr zobowiązani są przekazywać ABI na bieżąco informacje dotyczące nawiązania i rozwiązania stosunku pracy z pracownikami, którzy będą posiadać lub posiadają upoważnienie do przetwarzania danych osobowych.

§7

Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe powinien posiadać umiejętność bezpiecznej obsługi komputera i dobrą znajomość oprogramowania systemowego i operacyjnego, z którego będzie korzystał.

§8

1. Każdy nowo zatrudniany pracownik przed dopuszczeniem do obsługi systemu, w którym przetwarzane są dane osobowe zobowiązany jest zapoznać się z przepisami ustawy o ochronie danych osobowych, „Polityką Bezpieczeństwa", „Instrukcją zarządzania systemem informatycznym", a także winien być przeszkolony przez bezpośredniego przełożonego lub informatyka z oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będzie wykorzystywał przy realizacji zadań.
2. Wszyscy użytkownicy podlegają bieżącym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania).
3. Za organizację szkoleń, o których mowa w §8 odpowiedzialny jest Administrator Sieci Informatycznej.

§9

1. Do uwierzytelniania użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika np. biometrycznych.
2. Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

3. Identyfikatory dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela Administrator Sieci Informatycznej lub inna osoba upoważniona przez Administratora Danych.
4. Identyfikator użytkownika nie podlega zmianie.
5. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.
6. Pierwsze hasło dla użytkownika ustala Administrator Sieci Informatycznej przy wprowadzaniu identyfikatora użytkownika do systemu.
7. Hasła muszą odpowiadać następującym wymogom:
   1) hasła składają się co najmniej z:
      a) dla poziomu bezpieczeństwa podstawowego 6 znaków,
      b) dla poziomu bezpieczeństwa podwyższonego i wysokiego 8 znaków, i powinny zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   2) nie mogą być zapisywane w systemie w postaci jawnej,
   3) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania hasła przez osoby nieupoważnione,
   4) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

§10

1. Po otrzymaniu pierwszego hasła użytkownik zobowiązany jest zalogować się do systemu i powinien zmienić hasło. Przy wpisywaniu, hasło nie może być wyświetlane na ekranie.
2. Hasło zmieniane jest nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.

§11

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

§12

1. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł Administratora Sieci Informatycznej, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Administratora Danych.
2. Tryb przechowywania i udostępniania haseł Administratora Sieci Informatycznej określa **załącznik nr 2 do Instrukcji**. Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

ROZDZIAŁ V

Rejestrowanie i wyrejestrowywanie użytkowników zbiorów danych osobowych

§13

1. Ewidencję użytkowników zbiorów danych osobowych w Starostwie prowadzi Administrator bezpieczeństwa Informacji. Wzór ewidencji osób upoważnionych do dostępu do danych osobowych i obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych stanowi **załącznik nr 3 do Instrukcji.**
2. Ewidencja zawiera:
   1) nazwę zbioru danych osobowych,
   2) imię i nazwisko użytkownika,
   3) datę nadania upoważnienia,
   4) datę utraty upoważnienia,
   5) zakres upoważnienia,

6) identyfikator użytkownika (login),

7) uwagi (np. przyczyny utraty upoważnienia).

3. Postanowienia ust. 2 pkt. 4 nie dotyczą użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.

4. Ewidencja użytkowników może być prowadzona w systemie informatycznym.

§14

Nośniki magnetyczne (optyczne), na których gromadzone są wykazy zawierające ewidencję użytkowników przechowywane są w wyznaczonych szafach lub sejfach, do których mają dostęp wyłącznie: Administrator Bezpieczeństwa Informacji, Administrator Sieci Informatycznej lub osoba upoważniona przez Administratora Danych.

§15

1. Zmiany dotyczące użytkownika, takie jak:

1) zmiana imienia lub nazwiska,

2) zmiana zakresu upoważnienia, podlegają niezwłocznemu odnotowaniu w ewidencji, o której mowa w Instrukcji.

§16

1. Zmiany dotyczące użytkownika takie jak:

1) rozwiązanie umowy,

2) utrata upoważnienia do dostępu do danych osobowych,

3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,

powodują wyrejestrowanie użytkownika przez Administratora Sieci Informatycznej w trybie natychmiastowym, z ewidencji, o której mowa w Instrukcji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

§17

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. Administrator Sieci Informatycznej, zobowiązany jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie oznaczenia.

§18

Dane dotyczące osób, które zostały wykreślone z ewidencji użytkowników, z przyczyn, których mowa w Instrukcji, są gromadzone w postaci odrębnych zbiorów archiwalnych lub stosuje się odpowiednie ich oznaczenia.

ROZDZIAŁ VI

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§19

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

§20

W przypadku stwierdzenia, bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik zobowiązany jest postępować zgodnie z zasadami określonymi w „Polityce Bezpieczeństwa".

§21

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika.

3. Jeśli system to umożliwia, po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.

§22

1. Przed opuszczeniem stanowiska pracy, użytkownik zobowiązany jest:
   1) wylogować się z systemu informatycznego lub
   2) poczekać, aż aktywuje się blokowany hasłem wygaszacz ekranu.

§23

1. Kończąc pracę należy:
   1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetycznie i optyczne, na których znajdują się dane osobowe, mając na uwadze zasadę tzw. „czystego biurka".
   3) w uzasadnionych przypadkach Administrator Sieci Informatycznej może nakazać użytkownikom pozostawienie włączonego sprzętu komputerowego, po uprzednim wylogowaniu się z systemu informatycznego.

ROZDZIAŁ VII

Procedury tworzenia kopii zapasowych

§24

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów,

powinny być odpowiednio oznakowane i przechowywane w wyznaczonych odpowiednio zabezpieczonych pomieszczeniach.

2. Kopie zapasowe określone w ust. 1 niniejszego paragrafu powinny być sporządzane regularnie w okresach wyznaczonych w **załączniku nr 4 do instrukcji.**

3. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie odpowiedzialny jest Administrator Sieci Informatycznej.

4. ASI odpowiada także za sprawdzanie poprawności wykonywania kopii zapasowych na nośnik zewnętrzny.

5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§25

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.

2. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje Administrator Sieci Informatycznej. Z czynności zniszczenia ASI sporządza notatkę.

3. Z nośników magnetycznych i optycznych wielokrotnego użytku np., CDRW, DVD-RW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.

4. Dane zawarte na nośnikach optycznych jednokrotnego użytku np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VIII

Przechowywanie danych osobowych

§26

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.

2. W wypadku przekazywania urządzeń lub nośników zawierających dane osobowe, tzw. „wrażliwe", o których mowa w art.27 ust ustawy o ochronie danych osobowych, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:

   a) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub

   b) stosowanie metod kryptograficznych, lub

   c) stosowanie odpowiednich zabezpieczeń fizycznych, lub

   d) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

3. Kartoteki powinny być przechowywane w zamkniętych szafach, znajdujących się w wyznaczonych odpowiednio zabezpieczonych pomieszczeniach.

4. Wydruki robocze błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

5. Szczegółowy opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w „Polityce Bezpieczeństwa".

§27

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji dokumentów.

2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§28

Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Administrator Danych na wniosek Administratora Bezpieczeństwa Informacji.

§29

1. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:

   a) datę dokonania likwidacji,

   b) przedmiot likwidacji (nośniki, kartoteka),

   c) przedział czasowy likwidowanych zbiorów danych osobowych,

   d) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ IX

Zabezpieczenie systemu informatycznego

§30

1. System informatyczny zabezpiecza się przed:

   1) działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

2) utratą danych spowodowaną:

a) działaniem nieautoryzowanego oprogramowania,

b) awarią zasilania lub zakłóceniami w sieci zasilającej.

§31

1. Administrator Sieci Informatycznej odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowana zabezpieczającego system informatyczny.
2. Nowe wersje oprogramowania instaluje wyłącznie Administrator Sieci Informatycznej, niezwłocznie po ich otrzymaniu lub osoba upoważniona przez ASI.
3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Administrator Bezpieczeństwa Informacji.

§32

1. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.
2. Program antywirusowy należy instalować również na komputerach przenośnych.

§33

W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§34

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych, optycznych służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów instalacyjnych.

2. Na serwerach, w miarę możliwości technicznych oprogramowanie antywirusowe powinno być aktywne cały czas.

3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomianego pliku.

§35

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.

§36

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora Sieci Informatycznej.

2. Administrator Sieci Informatycznej usuwa wirusa, jeśli automatycznie nie dokonał tego program.

§37

W razie niemożności usunięcia wirusa, Administrator Sieci Informatycznej za zgodą Administratora Danych, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.

§38

1. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.

2. Prace określone w ust. 1 są wykonywane pod nadzorem Administratora Sieci Informatycznej lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.

§39

1. Administrator Sieci Informatycznej jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.

2. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i dyskietkach.

§40

Po usunięciu wirusa Administrator Sieci Informatycznej sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.

§41

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego, system informatyczny służący do przetwarzania danych, chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
   1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
   2) kontrolę działań inicjowanych z sieci publicznej do systemu informatycznego.
3. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

§42

Wyrażone w niniejszym rozdziale zabezpieczenia mają zastosowanie także do przypadków awarii systemu, spowodowanych błędem programu bądź użytkownika.

ROZDZIAŁ X

Wymagania dotyczące sprzętu i oprogramowania

§43

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.

2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.

3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępniać komputera osobom nieupoważnionym.

§44

1. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.

2. Sieć komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewnić bezpieczne wyłączanie systemu informatycznego, po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.

3. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie napięcia przez minimum 15 minut oraz na wykonanie bezpiecznego wyłączenia serwera, tak by przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.

§45

1. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

2. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, modemy) powinny być w miarę możliwości technicznych, włączone do wydzielonej sieci energetycznej, zapewniającej odpowiednie uziemienie i zabezpieczenie przed przepięciami.

3. Gniazda zasilania sieci komputerowej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników lub wykonane w specjalnym standardzie.

§46

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.

2. Dane osobowe przesyłane po łączach telekomunikacyjnych wewnątrz danej sieci, powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.

3. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnętrz powinny być w miarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.

§47

Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

§48

Administrator Sieci Informatycznej odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.

§49

1. Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
2. Ekrany monitorów, powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
3. Za spełnienie obowiązku określonego w ust. 2 odpowiadają użytkownicy i kierownicy komórek organizacyjnych.

§50

1. Administrator Sieci Informatycznej jest odpowiedzialny za to, aby dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu,
   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
   3) źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą,
   4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione,

5) dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

6) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

Wymagania określone w niniejszym ustępie nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt a i b, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust 1 pkt. d, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

5. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie:

   1) daty pierwszego wprowadzenia danych,

   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

6. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w ust. 1 pkt. 3) 4) 5), należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

ROZDZIAŁ XI

Procedury wykonywania przeglądów i konserwacji

§51

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych niewymagających angażowania zewnętrznych firm serwisowych dokonuje Administrator Sieci Informatycznej.
2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z ich zakresami upoważnień i odpowiedzialności.

§52

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Administratora Danych przez uprawnionych przedstawicieli tych firm pod nadzorem Administratora Sieci Informatycznej lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.

§53

1. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania i przechowywania danych osobowych należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.
2. Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić w sposób uniemożliwiający ich odczytanie.

§54

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Administrator Sieci Informatycznej lub osoba wyznaczona przez Administratora Danych.

RODZIAŁ XII

Postanowienia końcowe

§55

Instrukcja jest dokumentem wewnętrznym i nie może być udostępniona osobom trzecim w żadnej formie.

§56

Kierownicy komórek organizacyjnych są zobowiązani zapoznać z treścią Instrukcji każdego użytkownika.

§57

1. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji.

STAROSTA
Jan Zychliński

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA* Nr .....
do przetwarzania danych osobowych
w systemie informatycznym lub w zbiorze w wersji papierowej

Z dniem ..... upoważniam/anuluję Upoważnienie Nr .....*
(data)
Panią/Pani/Pana*.....,
(nazwisko i imię)
pracownika .....,
(nazwa komórki organizacyjnej)

a) **do obsługi systemu informatycznego**: .....
(nazwa systemu lub programu)
w zakresie: ..... danych osobowych.
(wglądu, wprowadzania, przechowywania, modyfikacji, usuwania itp.)

b) **do obsługi zbioru w wersji papierowej**: .....
(nazwa zbioru)
w zakresie: ..... danych osobowych.
(wglądu, wprowadzania, przechowywania, modyfikacji, usuwania itp.)

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

.....
(miejscowość i data)

.....
(pieczęć i podpis Administratora Danych)

Wypełnia Administrator Sieci Informatycznej:

Identyfikator użytkownika: .....

Data zarejestrowania w systemie: .....**

Data wyrejestrowania użytkownika
(zablokowania dostępu) z systemu: .....***

Podpis ASI: .....

*) niepotrzebne skreślić
**) wypełnić w przypadku wydania upoważnienia
***) wypełnić w przypadku anulowania upoważnienia

TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ ADMINISTRATORA SIECI INFORMATYCZNEJ

Ustala się następujący tryb postępowania z hasłami ASI:

1. Hasła Administratora Sieci Informatycznej przechowywane są formie pisemnej w zapieczętowanej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada wyłącznie Starosta i osoby przez niego upoważnione.
3. Hasła, o których mowa w pkt. 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Hasta zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inne nieupoważnione osoby.
5. Nowe, aktualne hasto zabezpiecza się według procedur opisanych w pkt 1 i 2.
6. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów.
7. Niszczenia, a którym mowa w pkt 6 dokonuje Administrator Sieci Informatycznej w obecności Starosty lub osoby przez niego upoważnionej.
8. W sytuacji kryzysowych pod nieobecność Administratora Sieci Informatycznej lub w razie jego niedyspozycji Starosta udostępnia hasło osobie przez siebie wyznaczonej.

.....

podpis Administratora Danych

Wyłącznie do użytku wewnętrznego
Załącznik Nr 3 do Instrukcji zarządzania systemem informatycznym
Zarządzenie Nr 95 / 2012 z dnia 18 grudnia 2012 r.

Lp.	Nazwa zbioru danych(1)	Nazwisko i Imię użytkownika	Nazwa identyfikatora (login)	Rodzaj (zakres) uprawnień (2)	Data nadania upoważ.	Data utraty upoważ.	Lokalizacja (nazwa KO, nr pokoju)	Uwagi
1.								
2.								
3.								
4.								
5.								

(1) nazwa zbioru danych i/lub systemu, itp.

(2) Skróty stosowane do określenia uprawnień:
P – prawo do przeglądania danych na ekranie i drukowania danych
Z – prawo do zmiany danych
D – prawo do dopisywania danych
U – prawo do usuwania danych
N – prawo do zakładania nowych kont/aktualizacji Planu Kont
O/Z – prawo do otwierania/ zamykania miesiąca/roku
A/W – prawo do akceptacji/wysyłania
A – prawo do wykonywania kopii archiwalnych

Dane aktualne na dzień: ...../...../.....

Data i podpis ABI: .....

CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH

Ustala się następującą. częstotliwość tworzenia kopii na nośnikach zewnętrznych-magnetycznych I optycznych:

1. Kopie dobowe 1 tygodniowe, wykonywane są. przez Administratora Sieci Informatycznej lub użytkowników obejmujące serwery danych.
2. Kopie miesięczne, umieszczane w zapieczętowanych kopertach, deponowane przez Administratora Systemu Informatycznego w miejscu w §26 instrukcji obejmujące:
    a. serwery danych,
    b. stacje robocze.
3. Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych.
4. Niszczenie kopii awaryjnych należy wykonywać w sposób określony w Instrukcji.
5. W sytuacjach awaryjnych zaistniałych pod nieobecność Administratora Sieci Informatycznej lub w razie jego niedyspozycji Starosta udostępnia kopie awaryjne osobie przez siebie wyznaczonej.

.....

podpis Administratora Danych