I N S T R U K C J A ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Postanowienia ogólne

§ 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 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).

§ 2

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

§ 3

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 lub 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 wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,

5) Administratorze Danych - rozumie się przez to Starostwo Powiatowe w Wąbrzeźnie reprezentowany przez Starostę,

6) Staroście - rozumie się przez to Starostę Wąbrzeskiego,

7) Administratorze Bezpieczeństwa Informacji - rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych,

8) osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację - rozumie się przez to wyznaczonego przez Starostę informatyka odpowiedzialnego za powyższe zadania, zwanego dalej „Administratorem Systemu Informatycznego",

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

10) użytkowniku - rozumie się przez to osobę upoważnioną przez Starostę lub osobę przez niego wyznaczoną, do przetwarzania danych osobowych w systemie informatycznym oraz kartotekach,

11) pracowniku ochrony - rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych,

12) 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 lub gromadzone w kartotekach.

§ 4

1. 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.

2. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
3. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:

1) poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,

2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,

4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

4. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek oraz osoby na stanowiskach samodzielnych.

§ 5

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

1) podstawowy,

2) podwyższony,

3) wysoki.

2. Poziom co najmniej podstawowy stosuje się, gdy:

1) w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy o ochronie danych osobowych, oraz

2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

3. Poziom co najmniej podwyższony stosuje się, gdy:

1) w systemie informatycznym są przetwarzane dane, o których mowa w art. 27 ustawy o ochronie danych osobowych, oraz

2) 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. W systemach informatycznych administratora danych stosuje się poziom bezpieczeństwa wysoki.

§ 6

Realizację zamierzeń określonych w § 4 powinny zagwarantować następujące założenia:

1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania 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 różnych poziomów zbiorów danych osobowych - stosownie do indywidualnego zakresu upoważnienia,

4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,

5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,

6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,

7) 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.

ROZDZIAŁ II
Przydział uprawnień i identyfikatorów

§ 7

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie. Wzór upoważnienia do przetwarzania danych osobowych, 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 użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.
5. Administrator Systemu Informatycznego na wniosek kierownika komórki organizacyjnej użytkownika definiuje poziom uprawnień użytkownika określony w ust 3 niniejszego paragrafu.
6. Jeśli zakres wnioskowanych przez kierownika komórki organizacyjnej uprawnień dla użytkownika wykracza w ocenie Administrator Systemu Informatycznego poza określony w ust. 3 powyżej, Administrator Systemu Informatycznego zgłasza ten fakt do Administratora Bezpieczeństwa Informacji, który w razie potrzeby decyduje o ostatecznym zakresie uprawnień.
7. Administrator Systemu Informatycznego może opracować formularz wniosku określonego w ust. 5 powyżej oraz zobowiązany jest do prowadzenia ewidencji przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do danych osobowych przetwarzanych w systemie informatycznym oraz dokonywaniem zmian w zakresie przyznanych uprawnień.

§ 8

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

§ 9

1. Każdy użytkownik - przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe - podlega przeszkoleniu w zakresie:

    1) obsługi komputera, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, które będzie wykorzystywał,

    2) przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.

2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§ 10

1. Za organizację szkoleń, o których mowa w § 9 odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
2. Szkolenia odbywają się na wniosek kierowników komórek organizacyjnych.

§ 11

Do uwierzytelniania użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika.

§ 12

Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

§ 13

1. Identyfikatory dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela Administrator Systemu Informatycznego lub inna osoba upoważniona przez Administratora Danych.

Identyfikator użytkownika nie podlega zmianie.

Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

§ 14

Pierwsze hasło dla użytkownika ustala Administrator Systemu Informatycznego lub upoważniona przez niego osoba przy wprowadzaniu identyfikatora użytkownika do systemu.

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 haseł przez osoby nieupoważnione,

4) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

5) nie mogą być używane poza systemem informatycznym Administratora Danych.

§ 15

1. Po otrzymaniu pierwszego hasła użytkownik zobowiązany jest zalogować się do systemu i zmienić hasło, jeżeli system umożliwia takie działanie. 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.

§ 16

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

§ 17

1. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł Administratora Systemu Informatycznego, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Administratora Bezpieczeństwa Informacji.
2. Tryb przechowywania i udostępniania haseł Administratora Systemu Informatycznego określa załącznik nr 2 do Instrukcji.

ROZDZIAŁ III Rejestrowanie i wyrejestrowywanie użytkowników

§ 18

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi osoba wyznaczona przez Administratora Danych.

   Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych, stanowi załącznik nr 3 do Instrukcji.

2. Ewidencja zawiera:
   1) imię i nazwisko użytkownika,
   2) datę nadania i ustania upoważnienia,
   3) zakres upoważnienia,
   4) identyfikator użytkownika.
3. Postanowienia ust. 2 pkt 4) nie dotyczą użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych może być prowadzona w systemie informatycznym i jest dostępna dla wszystkich użytkowników.

§ 19

Nośniki danych, na których gromadzone są kopie wykazów zawierających ewidencję przyznanych poszczególnym użytkownikom uprawnień przechowywane są w szafach lub sejfach, do których mają dostęp wyłącznie osoby wyznaczone przez Administratora Danych.

§ 20

Zmiany dotyczące użytkownika, takie jak:

1) zmiana imienia lub nazwiska,

2) zmiana zakresu upoważnienia,

podlegają niezwłocznemu odnotowaniu w ewidencji, o której mowa w § 18 Instrukcji.

§ 21

1. Zmiany dotyczące użytkownika, takie jak:

   1) rozwiązanie umowy,

   2) utrata upoważnienia do przetwarzania danych osobowych,

   3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,

   powodują wyrejestrowanie użytkownika z ewidencji przez osobę, o której mowa w § 18 Instrukcji oraz zablokowanie przez Administratora Systemu Informatycznego identyfikatora oraz unieważnienie hasła tego użytkownika.

2. Kierownicy komórek organizacyjnych oraz osoba odpowiedzialna za sprawy kadrowe w przypadku osób na samodzielnych stanowiskach odpowiadają za natychmiastowe zgłoszenie do osoby wyznaczonej przez Administratora Danych o której mowa § 18 Instrukcji, użytkowników, którzy utracili uprawnienia do przetwarzania danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji użytkowników, o której mowa w § 18 Instrukcji.

§ 22

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. Osoba prowadząca ewidencję, o której mowa w § 18 Instrukcji, obowiązana jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenia.

§ 23

Dane dotyczące osób, które zostały wykreślone z ewidencji osób upoważnionych do przetwarzania danych osobowych, z przyczyn, których mowa w § 21 ust. 1 Instrukcji, są

gromadzone w postaci odrębnych zbiorów archiwalnych lub stosuje się odpowiednie ich oznaczenia.

ROZDZIAŁ IV Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§ 24

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany 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.

§ 25

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie poufności danych osobowych, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa danych osobowych zwanej dalej „Polityką".

§ 26

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.

3. Użytkownik wprowadza identyfikator i dokonuje uwierzytelnienia.

4. Jeśli system to umożliwia, po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
5. Administrator Systemu Informatycznego ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną.

§ 27

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:

1) wylogować się z systemu informatycznego lub,

2) poczekać, aż zaktywizuje się blokowany hasłem wygaszacz ekranu.

§ 28

Kończąc pracę należy:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

ROZDZIAŁ V
Procedury tworzenia kopii zapasowych

§ 29

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych 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 Systemu Informatycznego.
4. Odpowiada on także za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.
5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§ 30

1. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych, o ile zostali do tego upoważnieni przez Administratora Systemu Informatycznego.

2. Użytkownicy określeni w ust. 1 są odpowiedzialni za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie.

§ 31

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.
2. Zniszczenia kopii zapasowych dokonuje Administrator Systemu Informatycznego w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego wyznaczonej.
3. Z nośników danych wielokrotnego użytku 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 jednokrotnego użytku należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VI
Przetwarzanie danych osobowych

§ 32

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, zwłaszcza tzw. „wrażliwe", o których mowa w art. 27 ust. 1 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:

    1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub
    2) stosowanie metod kryptograficznych, lub
    3) stosowanie odpowiednich zabezpieczeń fizycznych, lub
    4) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

3. Dane osobowe zapisywane na nośnikach zewnętrznych tworzące kopie zapasowe kolejnych okresów, powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
4. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
5. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
6. Szczegółowy opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce bezpieczeństwa.

§33

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.

§34

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

§35

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:

1) datę dokonania likwidacji,
2) przedmiot likwidacji (nośniki, kartoteka),
3) przedział czasowy likwidowanych zbiorów danych osobowych,
4) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ VII
Zabezpieczenie systemu informatycznego

§ 36

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.

§ 37

1. Administrator Systemu Informatycznego odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania.
2. Nowe wersje oprogramowania instaluje wyłącznie Administrator Systemu Informatycznego lub upoważnione przez niego osoby niezwłocznie po ich otrzymaniu.
3. Administrator systemu Informatycznego odpowiada za kontrolę czy autorzy oprogramowania określonego w załączniku nr 2 dostarczyli dokumentację zawierającą opis struktury zbiorów danych osobowych wraz ze wskazaniem poszczególnych pól informacyjnych i powiązań między nimi.
4. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania dokonuje Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

§ 38

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.

§39

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

§40

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i 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 uruchamianego pliku.

§41

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

§42

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora Systemu Informatycznego.
2. Jeśli program antywirusowy automatycznie nie usunął wirusa Administrator Systemu Informatycznego usuwa wirusa oraz informuje Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.

§43

W razie niemożności usunięcia wirusa, Administrator Systemu Informatycznego za zgodą Administratora Bezpieczeństwa Informacji, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.

§ 44

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 Systemu Informatycznego lub upoważnionej przez niego osoby i w miarę możliwości bez dostępu do danych osobowych.

§ 45

1. Administrator Systemu Informatycznego jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.
2. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i używanych nośnikach danych.

§ 46

1. Po usunięciu wirusa w trybie określonym w § 42 ust 2 Administrator Systemu Informatycznego sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.
2. Administrator Systemu Informatycznego sporządza raport o wystąpieniu wirusa. Raport winien zawierać następujące informacje:
    1) nazwę wirusa,
    2) datę wykrycia wirusa,
    3) miejsce zainfekowania,
    4) źródło infekcji.
3. Raport, o którym mowa w ust. 2 przekazywany jest Administratorowi Bezpieczeństwa Informacji lub osobie przez niego wyznaczonej wraz z wnioskami, stosownymi do zaistniałej sytuacji.

§ 47

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych 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 i systemu informatycznego.
3. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

§ 48

Administrator Systemu Informatycznego prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów określonych w § 46 ust. 2.

§ 49

Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkownika.

ROZDZIAŁ VIII
Wymagania dotyczące sprzętu i oprogramowania

§ 50

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 udostępnić komputera osobom nieupoważnionym.

§ 51

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 aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
4. Zasilaczem awaryjnym powinna być zabezpieczona, co najmniej jedna stacja robocza.

§ 52

1. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest Administrator Systemu Informatycznego.
2. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
3. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, router-y, switch-e itd.) powinny być w miarę możliwości technicznych, włączone do wydzielonej sieci energetycznej, zapewniającej odpowiednie uziemienie i zabezpieczenie przed przepięciami.
4. Gniazda zasilania sieci komputerowej powinny być w miarę możliwości odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników lub wykonane w specjalnym standardzie.

§ 53

1. Dane osobowe przesyłane na nośnikach 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 zewnątrz danej sieci powinny być w miarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.

§54

1. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
2. Wykaz programów wykorzystywanych do przetwarzania danych osobowych zawiera załącznik nr 2 do Polityki.
3. Za aktualizację załącznika nr 2 do Polityki w zakresie programów wykorzystywanych do przetwarzania danych osobowych odpowiada Administrator Systemu Informatycznego.

§55

1. Administratora Systemu Informatycznego odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.

2. System informatyczny wykorzystywany jest przez użytkowników wyłącznie w celach służbowych. Wyjątki od powyższej reguły możliwe są jedynie za wyraźną zgodą Administratora Danych.
3. System informatyczny może być monitorowany, w tym również z zastosowaniem specjalistycznego oprogramowania lub sprzętu, w celu rejestracji aktywności użytkowników oraz sposobu wykorzystywania systemu informatycznego przez użytkowników.

§56

1. Ekrany monitorów stacji roboczych 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.

§ 57

1. Administrator Systemu Informatycznego 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, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

   5) 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 1 i 2, 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 4, 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 i 5 należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

ROZDZIAŁ IX Procedury wykonywania przeglądów i konserwacji

§58

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje Administrator Systemu Informatycznego oraz upoważnione przez niego osoby.
2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami upoważnień i odpowiedzialności.
3. Administrator Systemu Informatycznego w uzasadnionych przypadkach może opracować dla poszczególnych zasobów informatycznych szczegółowe procedury techniczno - eksploatacyjne, które stanowią podstawę do eksploatacji danego zasobu informatycznego w sposób odmienny od określonego w niniejszej Instrukcji.
4. Procedury określone w ust. 3 mogą dotyczyć użytkowników oraz Administratora Systemu Informatycznego i osób upoważnionych przez Administratora Danych, które realizują np. prace techniczne i administratorskie w stosunku do poszczególnych zasobów informatycznych.

§59

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Administratora Bezpieczeństwa Informacji przez uprawnionych przedstawicieli tych firm pod nadzorem Administratora Systemu Informatycznego lub upoważnionej przez niego osoby i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

§ 60

1. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania lub 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.

§ 61

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Administrator Systemu Informatycznego.

ROZDZIAŁ X
Postanowienia końcowe

§ 62

Instrukcja jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

§ 63

1. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią Instrukcji każdego użytkownika.
2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
3. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, stanowi załącznik nr 5 do Instrukcji.
4. Oświadczenia przechowywane są w aktach osobowych.

§64

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

(podpis Administratora Danych)

Starosta
Krzysztof Mackiewicz

Załącznik nr la) do Instrukcji zarządzania systemem informatycznym

(imię i nazwisko) *(miejscowość, data)*

■ W Z Ó R -

UPOWAŻNIENIE

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

Upoważnienie obejmuje prawo wglądu, wprowadzania, modyfikowania i usuwania danych osobowych.

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

(podpis Administratora Danych)

*/- niepotrzebne skreślić

Załącznik nr lb) do Instrukcji zarządzania systemem informatycznym

(imię i nazwisko) *(miejscowość, data)*

- W Z Ó R (podpis Administratora Danych)

* - niepotrzebne skreślić

UPOWAŻNIENIE

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

Upoważnienie obejmuje prawo wglądu bez prawa do wprowadzania, modyfikowania i usuwania danych osobowych.

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

Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym

TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

Ustala się następujący tryb postępowania z hasłami Administratora Systemu Informatycznego:

1. Hasła Administratora Systemu Informatycznego przechowywane są w formie pisemnej w zapieczętowanej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada Administrator Danych i osoby przez niego upoważnione.
3. Hasła, o którym mowa w pkt 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Hasła zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inną, nieupoważnioną osobę.
5. Nowe, aktualne hasło 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, o którym mowa w pkt 6 dokonuje Administrator Systemu Informatycznego w obecności Administratora Danych lub osoby przez niego upoważnionej.
8. W sytuacjach awaryjnych zaistniałych pod nieobecność Administratora Systemu Informatycznego lub w razie jego niedyspozycji Administrator Danych udostępnia hasło osobie przez siebie wyznaczonej.

(podpis Administratora Danych)

Załącznik nr 3 do Instrukcji zarządzania systemem informatycznym

- WZÓR -

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

L.p.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login /identyfikator	Uwagi
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						

Zakres upoważnienia:

1 - osoby mające pełny dostęp do danych osobowych, tj. wgląd, wprowadzanie, modyfikacja, usuwanie:
2 — osoby o ograniczonym dostępie wyłącznie do wglądu do danych osobowych, np. sprzątaczki, praktykanci, itp.

(podpis osoby odpowiedzialnej zaprowadzenie ewidencji)

Załącznik nr 4 do Instrukcji zarządzania systemem informatycznym

CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH

Ustala się następującą częstotliwość tworzenia kopii awaryjnych:

1. Kopie dobowe i tygodniowe, wykonywane przez Administratora Systemu Informatycznego lub użytkowników obejmujące:
    a. serwery danych,
2. Kopie miesięczne, wykonywane na nośnikach zewnętrznych - magnetycznych lub optycznych umieszczane w zapieczętowanych kopertach, deponowane przez Administratora Systemu Informatycznego w miejscu określonym w § 29 Instrukcji obejmujące:
    i. serwery danych,
    ii. stacje robocze.
3. Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych.
4. Niszczenie kopii należy wykonywać w sposób określony w Instrukcji.
5. W sytuacjach awaryjnych zaistniałych pod nieobecność Administratora Systemu Informatycznego lub w razie jego niedyspozycji Administrator Danych udostępnia kopie awaryjne osobie przez siebie wyznaczonej.

(podpis Administratora Danych)

Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym

(imię i nazwisko) *(miejscowość, data)*

WZOR

OŚWIADCZENIE

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

Jednocześnie zobowiązuję się do ich przestrzegania.

(podpis osoby składającej oświadczenie)

*/ niepotrzebne skreślić